Mit Stellenmarkt



Anzeige
nur 1,– €/Jahr
Jetzt die besten .me Domains sichern!
united domains
THE DOMAIN PEOPLE
Infos unter: www.united-domains.de

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

10 Oktober 2008 € 5,50 H 10554

Tutorial:
Silverlight 2
Connectivity und Deployment

Business-Smartphones im Vergleich:

iPhone gegen alle

Blackberry Bold, HTC Touch Diamond, iPhone 3G, Nokia E71



Softwareentwicklung:
Ruby 1.9
Rich Ajax Platform

Neues Tutorial:
Linux mit Active Directory

Sicherheit:
Backtrack 3
Apaches Modsecurity

Videotelefonie perfektioniert:
Telepräsenz-Systeme

Energie-Benchmark:
SPECpower

3D jenseits von Microsoft:
OpenGL 3.0

Marktübersicht:
PC-Management





Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70 iX Magazin für professionelle Informationstechnik www.ix.de Oktober 2008
Heise

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Vom Nicht-böse-Sein

Kein kleines Geschenk, das sich Google gerade noch rechtzeitig zum Zehnjährigen überreicht hat. Zwar steckt der Anfang September veröffentlichte Browser Chrome noch in den Betaschuhen, aber die Attacke der kalifornischen Suchspezialisten auf Internet Explorer & Co. läuft – demnächst vielleicht auf der wahrscheinlich besten Werbeplattform der Welt: Googles spartanischer Homepage.

Dass die googlesche Browser-Nachricht als Leitartikel auf den Wirtschaftsseiten einer Tageszeitung taugt, hätte im vorigen Jahrhundert noch als Science-Fiction durchgehen können. Heute, gleichsam zehn Jahre nach Altavista, nimmt das Internet einen nicht unerheblichen Teil des Wirtschaftslebens ein, Tendenz immer noch steigend. Da kann man nicht genug wissen.

Don’t be evil, lautet das Firmenmotto. Erfunden hat es der Hauptentwickler von Gmail (in Deutschland Google Mail), Paul Buchheit, im Jahre 2001.[1] Wie die Verantwortlichen um Gründer Larry Page und Sergey Brin die Einwilligung in die Zensur chinesischer Suchergebnisse damit in Einklang bringen, ist fast ein Orwellismus: Immer noch besser, die Chinesen haben Zugriff auf von Google ausgewählte Informationen, als dass ihre Regierung sie ganz vom Internet abschneidet. Elliot Schrage, Vizepräsident für weltweite Kommunikation und öffentliche Angelegenheiten, hat vor dem US-Repräsentantenhaus zur „Anpassung an lokale Bedingungen“ gesagt: „We believe that our current approach to China is consistent with this mantra.“[2]

Wer Monopole liebt, muss Google lieben. Zu dieser Gruppe gehört das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht, denn es rät vom allgemeinen Gebrauch des Browsers ab. Datenschützer sind ohnehin alarmiert, denn die Sammelleidenschaft der Suchmaschinenbetreiber geht über das Speichern gesuchter Begriffe weit hinaus: Nutzer des hauseigenen Maildienstes sollen die richtige Werbung bekommen, und was mit den Gesundheitsdaten geschieht, die man bei Google Health speichern kann, weiß niemand außerhalb des Googleplex, wo man schwört: „We will never sell your data. You are in control.“ Das dürfte im Zweifelsfall eine datenhungrige Regierung wenig interessieren …

Ob Chrome sich durchsetzt, hängt nicht nur von der Platzierung auf der meistbesuchten Homepage der Welt ab. Die Benutzung muss einfach sein (ist sie), die aufgerufenen Seiten muss der Browser schnell anzeigen (es sieht ganz danach aus), und es darf keine Angst aufkommen, dass die Daten in die falschen Hände geraten – welche immer das sein mögen. Googles Geschäftsmodell ist es, über erfasste Daten Werbung an die richtigen Empfänger zu verschicken. Unwahrscheinlich, dass die Firma aufs Sammeln verzichtet. Unwahrscheinlich, dass die gläsernen Surfer auf datensammelfreiem Suchen bestehen, denn auf den kostenlosen Service wollen sie nicht verzichten.

Henning Behme

HENNING BEHME



[1]Wikipedias Motto-Eintrag: en.wikipedia.org/wiki/Don’t_be_evil; [2]Googles Zeugnis vor dem Repräsentantenhaus: googleblog.blogspot.com/2006/02/testimony-internet-in-china.html

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Oktober 2008



Marktübersicht: PCs zentral verwalten

Zu Recht belächelt wird die sogenannte „Turnschuh-Administration“: Wenn die IT-Abteilung jeden PC vor Ort verwalten muss, ist das personalaufwendig und fehlerträchtig. PC-Managementsoftware soll nicht nur alles billiger, sondern auch alles besser machen.

Seite 88

Neues Tutorial: Linux mit Active Directory

Als Verzeichnisdienst für Windows-Umgebungen kommt man um Active Directory nicht herum. Da kann man es auch gleich für Unix und Linux einsetzen und das veraltete NIS (ehemals Yellow Pages) ablösen. Eine Schritt-für-Schritt-Anleitung zur erfolgreichen Umstellung.

Seite 134



Web-2.0-Entwicklung mit Rich Ajax Platform



Eclipse’ Rich Client Platform hat sich zur Erstellung von Desktop-Anwendungen schnell etabliert. Die Rich Ajax Platform verspricht nicht nur die leichte Migration ins Web, sondern auch die parallele Entwicklung von Web-2.0- und Desktop-Applikationen.

Seite 142

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Apples iPhone im Business-Vergleich

Als Kult- und Trend-Accessoire ist Apples iPhone kaum zu toppen. Doch wie schlägt es sich gegenüber den Smartphones der Konkurrenz, wenn es um den Alltagseinsatz im Geschäftsleben geht? Ein Vergleich mit dem Blackberry Bold, HTCs Touch Diamond und Nokias E71.

Seite 34



3D-Schnittstelle modernisiert: OpenGL 3.0

Jenseits von Windows fristet Direct3D ein Schattendasein, bei den Nicht-Microsoft-Betriebssystemen ist der Grafikstandard OpenGL das Maß der Dinge. Der liegt jetzt in Version 3.0 vor und berücksichtigt endlich auch die Fähigkeiten moderner Grafikhardware.

Seite 106



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Haftung für WLAN-Bereitstellung

(Haftung für offenes WLAN; *iX* 8/08; S. 14/ *iX* 9/08; S. 18)

Wir haben zwar ein offenes WLAN, der WLAN Controller gibt den Zugang zum Internet erst nach Eingabe von Benutzernamen und Passwort frei. Wie ist denn diese Konstellation zu werten? Das, was nach Ansicht der Richter mit Verschlüsselung erreicht werden soll, wird auch mit diesem Konstrukt erreicht, oder? Muss ich das WLAN trotzdem verschlüsseln ? (Wir sind eine Klinik und bieten diesen Dienst kostenlos unseren Patienten an.)

WOLFGANG THOMA, VIA E-MAIL

Grundsätzlich ist die Frage, wie denn genau eine „Verschlüsselung“ aussehen soll, von den deutschen Gerichten noch nicht abschließend geklärt. Bis das der Fall ist, bewegen sich Betreiber von WLAN-Hotspots auf rechtlich wackligem Terrain. Letztlich sollten Sie sich davon leiten lassen, was effektiven Schutz vor unberechtigter Nutzung des Hotspots bietet und gleichzeitig im Einzelfall angemessen ist. Als öffentlicher und insbesondere gewerblicher Betreiber, der den Internetzugang einer Vielzahl von Personen (Patienten) zur Verfügung stellt, sollten sie ohnehin eine juristische Einschätzung einholen, welche Maßnahmen sie insofern treffen sollten/müssen. Ihr Haus dürfte sich an deutlich strengeren Maßstäben messen lassen müssen, als dies bei einem privaten Hotspot-Betreiber der Fall ist (was ja Gegenstand des von mir in der iX dargestellten Gerichtsverfahrens war). Gegebenenfalls trifft Sie künftig auch die Pflicht, Nutzerdaten erfassen und das Nutzerverhalten protokollieren zu müssen, da Ihr Haus als Telediensteanbieter/ISP angesehen werden könnte, den die Pflichten der sogenannte Vorratsdatenspeicherung treffen könnten.

Zurück zur Ausgangsfrage: Es geht dem Gesetzgeber und den Gerichten nicht um eine Verschlüsselung des Hotspots der Verschlüsselung wegen, sondern darum, dass der Betreiber des Hotspots für alles verantwortlich gemacht werden kann, was über seinen Internetzugang (den Hotspot) von ihm oder Dritten „angestellt wird“, wenn er nicht zumutbare Schutzmechanismen vor Missbrauch ergreift.

Ähnlich wie bei einer „schlechten“ Verschlüsselung wäre auch bei dem von Ihnen gewählten Weg eine „schlechte“, weil ohne großen Aufwand umgeh- oder knackbare, Nutzerberechtigungsabfrage nicht ausreichend.

Auch müssen Sie im eigenen Interesse darauf achten, dass Sie den Namen der (berechtigten) Nutzer (Patienten) protokollieren, damit im Zweifelsfall bei einer Rechtsverletzung durch einen solchen Nutzer nicht Ihr Haus, sondern eben der einzelne Nutzer (Patient) zur Verantwortung gezogen werden kann.

(Tobias Haar)

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Werte vertauscht

(OO-Programmierung: .Net Framework 3.5 SP1; *iX* 9/08; S.108)

Leider scheint es mir so, als ob da etwas durcheinander geraten ist beim Vergleich der Persistence Frameworks. Die Aussagen im Text und in der Tabelle decken sich nicht immer. Ist dort ein Fehler unterlaufen oder habe ich ein Verständnisproblem? Das betrifft besonders den Punkt „Forward Engineering“.

GUIDO MÜLLER, VIA E-MAIL

Tatsächlich sind in der Spalte „Forward Engineering“ die Werte vertauscht. LINQ-to-SQL unterstützt dies, das ADO.NET Entity Framework nicht. (Holger Schwichtenberg)

Wichtige Plug-ins übersehen

(Blogging-Software: Sieben frei verfügbare Weblog-Systeme; *iX* 7/08; S. 42)

Als Serendipity/S9y-Benutzer hat mich die recht positive Erläuterung dieses Blog-Systems gefreut. In der Tabelle haben sich jedoch einige Fehler eingeschlichen.

So wird die Möglichkeit von Tags oder das Bloggen mittels Mail verneint. Beides ist jedoch über Plug-ins installierbar, ebenso die Möglichkeit von Revisionen oder die Moderation von Einträgen (die ebenfalls mit „nein“ angegeben sind). Auch die Podcastingfähigkeiten von S9y werden in der Tabelle als nicht vorhanden angegeben.

All diese Funktionen sind zwar nur mittels Plug-ins verfügbar. Aber es entspricht der Architektur von S9y, dass die meisten Funktionen nicht im Core, sondern als Plug-in nachrüstbar sind. So kommt auch die Grundkonfiguration von S9y mit etlichen Plug-ins zum Einsatz. Diese werden über den zentralen S9y-Webserver zur Online-Installation angeboten. Nachdem auch bei anderen Weblog-Systemen Plug-ins für ein „ja“ bei einzelnen Funktionen gesorgt haben, ist die Tabelle hier wohl als fehlerhaft zu bezeichnen.

Interessanterweise wird bei „Support“ ein „k. A.“ angegeben. Es hätte – nachdem sie www.s9y.org durchaus nennen – den Autoren jedoch auffallen müssen, dass unter www.s9y.org/forums ein entsprechendes Supportforum vorhanden ist, das auch eine rege deutschsprachige Community beheimatet.

Es ist ein wenig schade, dass der positive Eindruck, den der Artikel vermittelt, durch eine Tabelle vermindert wird, die den Eindruck vermittelt, Serendipity wäre recht funktionslos.

ROBERT LENDER, VIA E-MAIL

Versteckte Datenreste bei Solid State Discs

(Diverse Meldungen zu Solid State Discs)

Bei herkömmlichen Festplatten können Daten aus Fragmenten wiederhergestellt werden, nachdem sie gelöscht wurden. Es gibt viele sicherere Löschmethoden, bei denen die entsprechenden Speicherbereiche mehrmals überschrieben werden, um die Fragmente unbrauchbar zu machen. Würden beim Löschen auf Solid State Discs keine Fragmente bleiben, könnten sensible Daten durch einfaches Löschen vernichtet werden. Für Sicherheit zu sorgen wäre sehr viel einfacher.

KONSTANTIN BÖRNER, VIA E-MAIL

Beim Löschen einer Datei überschreibt auch bei SSDs das Betriebssystem nur den Verzeichniseintrag. Man muss auch bei einer SSD die Daten selbst überschreiben, wenn man sie endgültig vernichten will (einmal sollte genügen). Das verkürzt allerdings die Lebensdauer der Solid State Disc.

Außerdem genügt es nicht unbedingt, nur die zur Datei gehörenden Blöcke zu „übertünchen“. Die sogenannten Wear-Leveling-Algorithmen, die die Lebensdauer der Flash-Chips erhöhen sollen, schreiben einen Datenblock nämlich nicht immer an dieselbe Stelle. Es kann also passieren, dass die Originaldaten erhalten bleiben, selbst wenn der Block aus der Sicht des Betriebssystems mit Nullen gefüllt ist. Sie müssten schon ***alle*** *freien Blöcke überschreiben – und das beeinträchtigt die Lebensdauer noch viel mehr. Kurz gesagt: Es ist empfehlenswerter, die Daten auf einer SSD zu verschlüsseln, wenn man sie vor unbefugten Zugriffen schützen will. (Michael Riepe)*

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Praxis hoch im Kurs auf der Informatica Feminale

Dem Baulärm zum Trotz

Patricia Jung



Dass Frauen trotz aller Widrigkeiten Spaß an Informatik haben, zeigte einmal mehr das von Sponsoren weitgehend unbeachtete Sommerstudium der Informatica Feminale in Bremen. Bei all den Klagen der Wirtschaft über den Fachfrauenmangel fragt man sich, warum aus deren Reihen nicht mehr Unterstützung und Interesse für solch offenkundig erfolgreiche Projekte kommt.

Jährlicher Girls' Day (siehe *iX*-Link), ein Frauenstudiengang Informatik, Mentoring-Programme, Kompetenzzentren und Konferenzen zur Frage der Gewinnung weiblichen Nachwuchses in Informatik, Technik- und Naturwissenschaften – und dennoch ernüchtern die Ergebnisse: Nur noch 16 Prozent der Studienanfängerinnen in der Informatik waren 2007 weiblich gegenüber 19 Prozent im Jahre 2000, die Anzahl der weiblichen Lehrlinge in IT-Berufen sank von 14 Prozent im Jahre 2002 auf 9 Prozent im vergangenen Jahr. Bei generell abnehmenden Studentenzahlen verschärft dies dem Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Bitkom) zufolge den Fachkräftemangel.

Schuld haben immer die anderen

Was tun? Der Bitkom weist die Verantwortung hierfür selbstredend Schulen und Hochschulen zu und vermeidet es, die Privatwirtschaft in die Pflicht zu nehmen. Dabei wirken gerade die Arbeitsbedingungen, bei der Aussicht auf einen Einzelkämpferinnenstatus angefangen über die branchenüblichen Überstunden oder das oft noch mangelnde Engagement vieler Firmen bei der Vereinbarkeit von Familie und Beruf, wenig stimulierend auf junge Frauen.

Dass Informatik-Studentinnen und IT-Praktikerinnen trotz mangelndem Sponsoring seitens der Wirtschaft und wechselvoller Unterstützung seitens der Hochschule Spaß am Metier haben und willens sind, einander beim Wissenserwerb und der Karriereförderung zu helfen, zeigte einmal mehr das 11. bundesweite Sommerstudium der Informatica Feminale, das Ende August / Anfang September 2008 an der Universität Bremen stattfand.

Mut zur Lücke und gute Stimmung

Aufgrund des lange Zeit unklaren Status der Bauarbeiten am Fakultätsgebäude stand erst fünf Wochen vor Beginn fest, dass dem Sommerstudium überhaupt Räumlichkeiten zur Verfügung standen. Wegen der Kürze der verbleibenden Zeit zeigte die Organisatorin und Informatica-Gründerin Veronika Oechtering Mut zur Lücke und rekrutierte ein 20 Frauen starkes Dozentinnenteam, von denen die meisten der Informatica bereits lange verbunden waren.

27 Kurse und Vorträge, hauptsächlich zu Selbstläuferthemen vergangener Jahre, hieß die Devise, flankiert von Kinderbetreuung, Sport- und Aktivitätsangeboten wie Geocaching. Die Rechnung ging auf: Obwohl jegliche explizite Werbeaktion im Vorfeld unterblieb und die einmonatige Anmeldefrist mehr als kurz war, kamen etwa 70 Teilnehmerinnen – die kleinste Informatica seit Bestehen zwar, doch weder dies noch die Baustellensituation trübte die gute Stimmung auch nur im Geringsten.

Das Kursangebot umfasste vor allem praktisch motivierte Themen: Sicherheit und Kryptografie, Rapid Prototyping, Datenvisualisierung und generatives Design, Flash, PostgreSQL, ein Roboter-Workshop, dazu Kurse zur Schulung von Managementkompetenzen.

Linux-Akademie war ausgebucht

Aus dem vergangenen Jahr erfolgreich übernommen wurde das Konzept einer Linux-Akademie, bestehend aus mehreren, maximal eintägigen und aufeinander aufbauenden Modulen, die – von den ausgefallenen Embedded-Linux-Kursen abgesehen – allesamt aus- und sogar überbucht waren. Neben Kommandozeilen- und Systemadministrationsgrundlagen ging es hier um Shell-Skripting, Softwarebau aus dem Quellcode und den Boot-Prozess. Neu hinzu kam ein Open-Source-Kolloquium, auf dem das OpenStreetMap-Projekt, die Monitoring-Software Munin (siehe S. 130), das Thema Embedded Linux und die neue, auf CakePHP und Joomla aufsetzende Informatica-Webseite vorgestellt wurden.

Die trotz aller Widrigkeiten exzellente Resonanz war denn auch der Hauptgrund für Veronika Oechtering, das Datum der 12. Informatica Feminale in Bremen bereits festzusetzen: Vom 7. bis 18. September 2009 soll das dann hoffentlich fertig umgebaute Mehrzweckhochhaus wieder 150 bis 250 informatikbegeisterten Frauen offen stehen. Ein idealer Anlaufpunkt für Firmen, die die Förderung weiblichen Nachwuchses tatsächlich ernst nehmen. (ka)



Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Datenschutzgipfel will nach Datenpannen handeln

Es ging um nicht weniger, als den Vollzug des Bundesdatenschutzgesetzes zu verbessern und es umfassend zu überarbeiten. Darauf einigte sich Anfang September der von Bundesinnenminister Schäuble einberufene Datenschutzgipfel mit Vertretern aus Bund und Ländern als Reaktion auf die Skandale der letzten Zeit um den regen Handel mit Kundendaten und Auskünften der Meldeämter. Wichtigstes Ergebnis: Adressdaten dürfen künftig nur noch mit Einwilligung der Betroffenen weitergegeben werden. Dieses Opt-in-Prinzip gilt bislang noch nicht für sogenannte Listendaten. Die Weitergabe von bestimmten personenbezogenen Daten für einen anderen Zweck als den, für den die Daten ursprünglich erhoben wurden, ist beispielsweise für Werbezwecke zulässig, wenn kein Grund zur Annahme eines entgegenstehenden Interesses des Betroffenen besteht. Ein umfassendes Verbot des Datenhandels wird es aber nicht geben. Dafür stehen aber höhere Bußgelder in Aussicht – und eine Gesetzesgrundlage für das Abschöpfen von Gewinnen aus rechtswidrigem Datenhandel. *Tobias Haar*

E-Mails auf anstößige und vertrauliche Bilder durchsuchen

Messagelabs übernimmt Fortium ICA (Image Composition Analysis), eine Tochterfirma von Fortium Technologies. Der Messaging-Dienstleister kauft damit die Technik auf, die bereits seit einigen Jahren im eigenen „Image Control Service“ zum Einsatz kommt und die verhindern soll, dass unerwünschte oder anstößige Bilder in ein Firmennetz gelangen beziehungsweise dieses verlassen oder dass vertrauliches Material in falsche Hände gerät.

Über finanzielle Details der Transaktion haben die Beteiligten Verschwiegenheit vereinbart. Seine Geschäftszweige DVD-Kopierschutz und Online-Medienanalyse zur Durchsetzung von Copyright-Ansprüchen wird Fortium Technologies unter dem gleichen Namen weiterführen. Mit Fortium ICA bestehende Lizenz- und Serviceverträge werden laut Messagelabs auch nach der Übernahme erfüllt.

Maschinen-Fernwartung über verschlüsselte Verbindungen

GeNUA bietet mit ihrer GeNUBox Fernwartungsmöglichkeiten für die Betreiber von Maschinen in abgelegenen Gebieten oder solche, die sich im mobilen Einsatz befinden. Die für den Einsatz in rauen Umgebungen konzipierte Appliance ist nicht nur übers Internet, sondern auch per Mobilfunk und Satellit erreichbar. Damit bietet sie sich für den Einsatz etwa in Windkraftanlagen oder in Schiffsmaschinenräumen an.



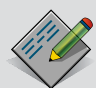
Für den Datenaustausch, beispielsweise die Übertragung von Betriebsdaten oder zu Wartungszwecken, nutzt die Appliance ein verschlüsseltes Virtual Private Network (VPN). Eine Demonstration plant GeNUA für die Münchener Systems (21. bis 24. Oktober 2008, Halle B3, Stand 321). Die GeNUBox gibt es in sieben Varianten, darunter die abgebildete 100C (ab 650 Euro).

Anzeige

SMTP-Erweiterungen für internationalisierte Mail-Header

Die Internet Engineering Task Force (IETF) hat Anfang September mit den als „experimental“ gekennzeichneten RFCs 5335 bis 5337 mögliche Grundlagen für international verwendbare E-Mail-Header mit lokalen Sonderzeichen aufgezeigt. Besonders fernöstliche Anwender leiden unter den derzeitigen Bedingungen für das Schreiben von E-Mails an internationalisierte Domains, da der Local Part (der Teil vor dem „@“) nach wie vor in herkömmlichem ASCII zu halten ist. Die neuen Vorschläge sehen vor, UTF8-kodierte Zeichen nicht nur in den Mailadressen, sondern auch anderswo im Header zu verwenden. Eine konkrete Umsetzung würde allerdings aufwendige Anpassungen aller beteiligten Systeme erfordern. Neben der Software für Mailserver (Sendmail, Postfix, Exim und Co.) und -clients (etwa Thunderbird oder Outlook) wären sämtliche Produkte betroffen, die Mails in irgendeiner Weise archivieren oder managen, zum Beispiel im Rahmen von Mailinglisten.





IT-Service-Management: Das i-doit-Projekt für IT-Dokumentation stellt eine Kopplung zur Netzüberwachungssoftware Nagios bereit. Admins müssen Überwachung und Dokumentation daher nicht mehr getrennt voneinander betrachten. Unter www.i-doit.org steht die Schnittstelle zur freien Verfügung.

Immer mehr Browser: Gomez, Inc., Dienstleister für die Performance-Analyse von Webangeboten, hat sein Angebot auf die neuen Browser von Google und Microsoft ausgedehnt. Laut Gomez haben viele Webseitenbetreiber Schwierigkeiten damit, zwei weitere Plattformen zu berücksichtigen (www.gomez.com).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

Command Center von Raritan steuert VMs

Virtuelle Maschinen auf Basis von VMware können Administratoren mit dem Command Center Secure Gateway 4.0 (CC-SG) von einer Konsole aus verwalten. Das Gerät von Raritan soll die gesamte Infrastruktur erfassen können, vom Power-Management über das Netzwerk bis hin zu den Servern. Dazu überwacht das CC-SG auch den Datenverkehr zwischen VMs und den physischen Plattformen.

Die sichtbaren Systeme und Komponenten kann der Administrator von seiner Konsole aus in Gruppen zusammenfassen, direkten Zugriff auf die Rechner und die Geräte erhält er über die systemspezifischen Verfahren, etwa per RDP, VNC oder SSH. Er kann zudem Techniken anderer Hersteller wie HPs iLo, IBMs RSA oder Dells DRAC nutzen. Sind intelligente Power Distribution Units (PDUs) vorhanden wie die Dominion PX von Raritan, kann der Systemadministrator über das Command Center automatisch Seriennummern sowie Firmware der PDUs und die Anzahl der schaltbaren Steckdosen erfassen. Anhand der gesammelten Daten über den aktuellen Stromverbrauch kann er entscheiden, welche wenig ausgelasteten Server er in eine VM verlagern und welche physischen Systeme er abschalten kann.

Verfügbar sind zwei Modelle: Das Command Center Secure Gateway V1 zum Preis ab 5012 Euro für 128 oder 256 Knoten, CC-SG E1 für die doppelte Menge gibt es ab 8796 Euro.



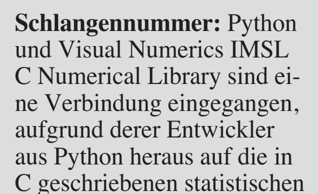
Im Blick: Mit Raritans Command Center kann der Administrator sowohl die VMS als auch die darunterliegende physische Schicht verwalten (Abb. 1).

Embedded-Systeme im Cyberspace

Unter dem doppelsinnigen Namen VIERforES (Virtuelle und Erweiterte Realität für höchste Sicherheit und Zuverlässigkeit von „Embedded Systems“) haben die Universitäten Magdeburg und Kaiserslautern sowie die beiden Fraunhofer-Institute IFF und IESE ein gemeinsames Projekt aus der Taufe gehoben.

Wissenschaftler der beteiligten Institutionen testen die in Geräten eingebauten Computer und die darauf laufende Software in einer virtuellen Realität. Dazu zählen unter anderem DVD-Rekorder, Auto-Elektronik und Computertomographen.

Im Rahmen seiner Initiative „Spitzenforschung und Innovation aus den neuen Ländern“ schießt das Bundesministerium für Bildung und Forschung 7,5 Millionen Euro für das VIERforES-Projekt zu. In den nächsten zwei Jahren will der Bund sechs Forschungsprojekte in Ostdeutschland mit insgesamt 45 Millionen Euro fördern.



Schlangennummer: Python und Visual Numerics IMSL C Numerical Library sind eine Verbindung eingegangen, aufgrund derer Entwickler aus Python heraus auf die in C geschriebenen statistischen und mathematischen Funktionen der IMSL über DLLs oder Shared Libraries zugreifen können. PyIMSL ist lieferbar und für Lizenznehmer der IMSL C Library kostenlos. Wer es nutzen will, muss über IMSL V5.5 oder eine höhere Version verfügen.

iX-Link ix0810014

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Petaflops-Prototypen für PRACE

Nach eine Analysephase hat die europäische Initiative PRACE sechs Prototypen von Petaflops-Computern ausgewählt, mit deren Aufbau die Partner noch dieses Jahr beginnen wollen. Die Prototypen dienen dazu, Performance und Skalierbarkeit beim Einsatz von Anwendungen, die zu erwartenden Gesamtkosten sowie die Energieeffizienz zu untersuchen. Die sechs Partner sind:
– Das Barcelona Supercomputing Center (BSC) in Spanien beschafft ein System von IBM mit Power6- und Cell-CPUs, ein Hybrid-Cluster.
– Die französische Atomenergiebehörde (CEA) und das Forschungszentrum Jülich (FZJ) sollen sich gemeinsam Intels Xeon-Prozessoren von Typ Nahalem widmen. Bei CEA will man einen Prototyp von Bull aufbauen, am FZJ einen mit derselben Architektur, aber mehr Prozessoren.
– CSC, das finnische IT Zentrum für Wissenschaft und das schweizerische CSCS (Swiss National Supercomputing Centre) nehmen sich gemeinsam eine CRAY XT5 vor. Das MPP-System soll im CSC entstehen.
– Außerdem nutzt das FZJ seine BlueGene/P von IBM, ebenfalls ein MPP, für das Projekt.
– Im Höchstleistungsrechenzentrum Stuttgart (HLRS) setzt man sich mit einem gekoppelten System, bestehend aus NECs SX-9 und einem zweiten mit Intels x86-Prozessoren, auseinander.
– Die Netherlands Computing Facilities Foundation (NCF) evaluiert IBMs Power6 in einem Shared Memory Multiprocessor. Das System wird bei SARA Computing and Networking Services in Amsterdam installiert.

Zusätzlich untersuchen die Forscher im Rahmen des PRACE-Projekts Managementsoftware in verteilten Infrastrukturen, erproben den produktionsnahen Einsatz, bereiten Benchmarks für die zukünftigen Petascale-Systeme vor und unternehmen Versuche zur Optimierung und Skalierung von Programmbibliotheken sowie der Anwendungen selbst. Außerdem bereiten sie die technischen Spezifikationen für die Beschaffung der künftige Produktionssysteme im Rahmen von PRACE 2009 und 2010 vor.



Auf der Spielwiese: 2009 dürfen sich Entwickler und Nutzer von Computerspielen auf zwei Veranstaltungsorte einstellen: Die Games Con in Leipzig findet wieder statt und trotzt dem Bundesverband Interaktive Unterhaltungssoftware (BIU), dessen Mitglieder zur Gamescom nach Köln ziehen wollen. Der BUI besteht aus 12 namhaften Anbietern von E-Games: Atari, Activision, Eidos Interactive, Electronic Arts, Koch Media, Konami, Microsoft, Nintendo, Sony, Take 2 Interactive, THQ und Ubisoft.

Xeon-Speed: Mit dem überarbeiteten E0-Stepping im 45-nm-Fertigungsprozess senkt Intel die Leistungsaufnahme. Der 3,2 GHz schnelle Quad-Core X5482 (Harpertown) etwa braucht nur noch 120 W statt bisher 150 W. Die geänderte CPU-ID erfordert jedoch ein BIOS-Update.

Komplett: Gemeinsam bieten Univention und IBM für den Mittelstand ein zertifizierten System, bestehend aus einem Server von IBM aus der Reihe System x3650 und dem Univention Corporate Server (UCS) unter Linux, für 25 Nutzer für 3649 Euro an – einschließlich der Installation vor Ort durch einen regionalen IT-Dienstleister.

Sicher virtuell: VPN-1 Virtual Edition (VE) von Check Point Technologies Ltd. soll als Security Gateway virtuelle Applikationen schützen. Das Produkt ist über VARs und bei VMware erhältlich, die Preisstaffel beginnt bei 7500 US-$ für fünf VMs.

iX-Link ix0810014


Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

iX-Veranstaltungen

www.ix-konferenz.de.

Die Planung von Veranstaltungen ist ein recht langfristiges Geschäft. Darum geht es an dieser Stelle schon jetzt um das Jahr 2009: Im Februar starten neue Kerberos-Veranstaltungen. Eine neue Chance also für alle, die in diesem Jahr nicht zum Zuge kamen, weil die Workshops immer wieder im Nu ausgebucht waren.

Im Detail: Los geht's am 9. bis 11. Februar in Hamburg, es folgen Termine in Frankfurt/Main (4. bis 6. März), Stuttgart (18. bis 20. März) und Wien (27. bis 29. Juni). Wie aufmerksame Leser sofort festgestellt haben dürften, gibt es jetzt einen optionalen dritten Workshop-Tag, der der Einbindung weiterer Netzdienste in die Single-Sign-On-Umgebung gewidmet ist. Dazu zählen Webserver, Maildienste, kerberisierte Netzdateisysteme und die in komplexen Windows-Netzen üblichen Active Directory Forests.

Weitere Informationen und das Anmeldeformular sind wie immer auf www.ix-konferenz.de zu finden.




Kerberos-Spezialisten der science + computing AG: Mark Pröhl (links) und Michael Weiser (rechts)

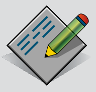
Microsofts Hyper-V-Strategie

Get Virtual now, rief Microsoft seinen Kunden auf dem Virtualisierungs-Gipfeltreffens in Bellevue (Washington, USA) zu und versprach, den Besuchern Expertenstatus zu verleihen. Konkret ging es um Microsofts Virtualisierer Hyper-V (Codename Viridian), einst Virtual Server 2008 genannt, für den sich die Redmonder Entwickler mit denen von Xen getroffen hatten. Der integrale Bestandteil des Windows Server 2008 Hyper-V liegt bis dato als RC2-Kandidat vor.

Für die Verwaltung der virtuellen Maschinen hat Microsoft den System Center Virtual Machine Manager 2008 als Nachfolger des bisherigen 2007er angekündigt. Zu den neuen Funktionen gehören unter anderem die Verwaltung von Clustern sowie der Multi Vendor Support, der es erlaubt, neben Hyper-V-Umgebungen auch virtuelle Maschinen auf VMwares ESX Server zu verwalten. Als besonderen Clou will Microsoft den Hyper-V Server 2008, eine auf die Virtualisierungsfunktionen reduzierte Betriebssystem-Variante, zum freien Download anbieten (www.microsoft.com/servers/hyper-v-server/default.mspx).

iX-Link ix0810016

KURZ NOTIERT



Ganz einfach: Wie Dell im Mai angekündigt hatte, bietet der PC-Hersteller unter dem Motto „We simplify IT" jetzt Systeme an, die für virtuelle Umgebungen optimiert sein sollen. Dazu zählen neue Blade- und Rack-Mount-Server, iSCSI-Speicher sowie der Support für Hyper-V, VMwares ESX 3.5 und Xen Server 5.0.

Abgenommen: Red Hat hat das israelische Softwarehaus Qumranet für 107 Millionen US-Dollar gekauft. Dessen kommerzieller Desktop-Virtualisierer SolidICE, der auf die freie Kernel Virtual Machine (KVM) aufsetzt, soll künftig fester Bestandteil von Red Hats Linux werden.

Suns Virtualisierungspaket xVM

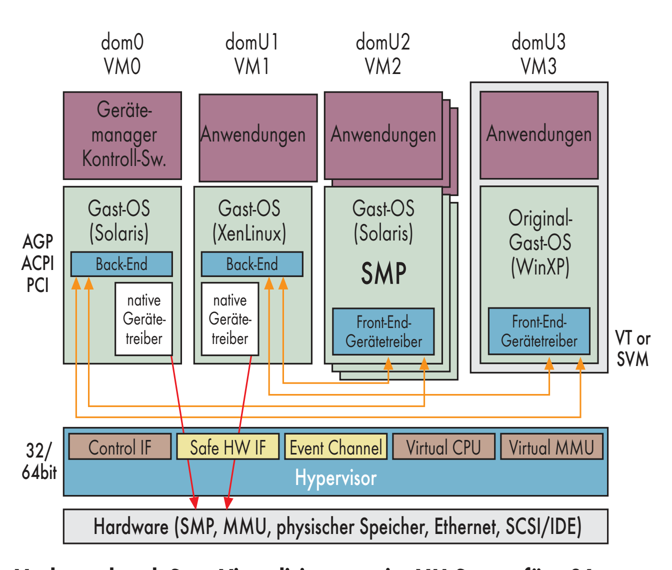
Nahezu zeitgleich mit Microsoft hat Sun Microsystems sein Virtualisierungspaket geschnürt. Unter xVM subsumiert der Hersteller Virtual Box 2.0, xVM Server, xVM Ops Center 2.0 und xVM VDI.

Mit der Version 2.0 der Virtual Box, in Suns Besitz seit der Übernahme von Innotec, kann der Anwender 64-Bit-Gastsysteme auf x64-Hosts betreiben. Sie nutzt Nested Page Tables (derzeit nur mit AMD-Prozessoren verfügbar) und das Command Queuing bei SATA-Platten. Die Version 2.0 unterstützt Images in Microsofts VHD-Format und stellt ein SDK mit Python-Schnittstelle für Linux und Solaris zur Verfügung. Außerdem hat Sun Apples Mac OS X (Leopard) ein eigenes, natives GUI spendiert sowie dessen Anbindung ans Netz verbessert.

Sun nutzt beim xVM Server im Unterschied zu anderen Xen-Implementierungen sein hauseigenes Betriebssystem Solaris x86 als Kontrollinstanz in der sogenannten Dom0. Damit stehen Anwendern spezielle Funktionen zur Verfügung wie das dynamische Filesystem ZFS und das Analysewerkzeug Dtrace. Suns xVM Server stellt die Betriebsmittel der physischen Plattform, die x86-CPUs, Haupt- und Massenspeicher sowie das Netzwerk virtuellen Maschinen unter Windows, Linux und Solaris zur Verfügung. Die Umgebung läuft auf Plattformen mit Intels und AMDs Prozessoren und nutzt deren Virtualisierungstechniken. Suns xVM Ops Center 2.0, ursprünglich als Managementsystem für Suns Server konzipiert, das sich zur Hardware-Überwachung sogar für ausgeschaltete Systeme auf deren ILOM stützt, kann darüber hinaus virtuelle Maschinen erkennen und verwalten.

Konsequent bleibt Sun bei seiner Strategie, seine Software als Open Source bereitzustellen. Interessenten können für den nichtkommerziellen Gebrauch die Quellen und die Binaries von xVM Server und xVM Ops Center frei herunterladen. Die Quellen stehen unter der GPL 3.0. Für Virtualbox 2.0 gilt die PUEL (Private Use and Evaluation License), für die Quellen GPL 2. Bei Suns xVM VDI muss man für den Download der Software einer speziellen Lizenz zustimmen, denn diese Komponente enthält unter anderem die Software der einstigen SCO-Tochter Tarantella. Das gesamte xVM-Paket soll laut Sun für den professionellen Einsatz lieferbar sein. Die Lizenzkosten gelten jeweils für ein Jahr pro physische Plattform: 500 US-Dollar für den xVM Server und 100 US-Dollar bis 350 US-Dollar für xVM Open Center, abhängig von der Zahl der zu verwaltenden Systeme.





Vorherrschend: Suns Virtualisierung mit xVM Server für x86-Architekturen nutzt Solaris in der Dom0.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

KURZ NOTIERT

IE 8 Beta 2: Microsofts Internet Explorer 8 liegt jetzt in einer zweiten Betaversion vor. Zu den Neuerungen gehört ein privater Surf-Modus, und die Adressleiste betont den Domainnamen, was verschleierte Adressen, wie beim Phishing üblich, erschwert.

XML-Editor: Altova hat eine Standard-Edition seines XML-Editor XMLSpy fertig, die inklusive Support für ein Jahr 123,75 € kostet; sie erlaubt das Editieren, Validieren und Betrachten von XML-Dokumenten. Zum Vergleich: Die Professional Edition kommt auf 498,75 € enthält dafür aber erheblich mehr, beispielsweise einen grafischen Schemadesigner (www.altova.com).

Neuer XML-Editor: Für 39 € bietet die Lüneburger Tooldriver Software ihren XML-Editor Edixs an. Er stellt Dokumente tabellarisch dar und erlaubt Copy & Paste zu und von Excel (www.tooldriver.de).

Semantic Web: Ontorprise und die CRG Information Services GmbH wollen die Semantic-Web-Tools erstgenannter Firma mit Microsofts Sharepoint-Server verbinden (www.ontoprise.de). Es handelt sich um den Semantic Gude, den Semantic Miner und die Mediawiki-Erweiterung Semantik Mediawiki+ (SMW+).

See-Rechenzentren: Google hat einen Patentantrag für Serverfarmen auf offener See eingereicht. Grund sind die riesigen Vorräte an Kühlwasser, vielleicht auch die Lage außerhalb von Hoheitsgewässern. Den nötigen Strom sollen die RZs selbst erzeugen.

iX-Link ix0810018

Diskussion um Googles Browser Chrome

Galvanisch



Henning Behme

Neue Browser braucht das Land – oder wenigstens einen, könnten sich Googles Entwickler gedacht haben. Und er soll, wenig überraschend, besonders gut für Webanwendungen wie Web-E-Mail sein.

Anfang September hat Google eine unter Windows XP (SP2) und Vista lauffähige Betaversion seines Webbrowsers Chrome zum Download freigegeben (www.google.com/chrome). Schnell hatten die ersten Surfer die Geschwindigkeit geprüft und für ausreichend befunden sowie die Datensammelwut kritisiert.

Die Chrome-eigene ID für jede Instanz der Software sowie die Tatsache, dass sie als Referenz für Kommunikation mit Google dient, erregte ebenso Unmut wie die Konzentration von Daten. BSI-Sprecher Matthias Gärtner brachte es angesichts dessen auf den Punkt: „Wenn ich mich von einem Anbieter abhängig mache, ist das Risiko höher.“ Das BSI riet insgesamt von der Benutzung des Browsers ab.

Dass Chrome die Option bietet, für einen der Tabs einen Inkognito-Modus einzustellen und so den Verlauf, Passwörter, Cookies et cetera dieser Mini-Sitzung anschließend automatisch zu löschen, gilt vielen als nicht hinreichend, weil es gerade von unerfahrenen Surfern zu viel voraussetze.

Was Chrome mit sich bringt

Googles Browser ist laut Hersteller ein Open-Source-Produkt, obwohl bislang noch kein Quellcode offengelegt ist. Vielleicht ändert sich das erst, wenn die Versionen für Linux und Mac OS X in einigen Monate kommen.

Chrome nutzt mit Webkit Software, die auch in Apples Safari steckt. Und mit der Freigabe des Quelltextes könnten andere Entwickler das von Google Erarbeitete prüfen – unter anderem daraufhin, ob nicht diese oder jene Eigenschaft in anderen Browser ebenfalls sinnvoll wäre.

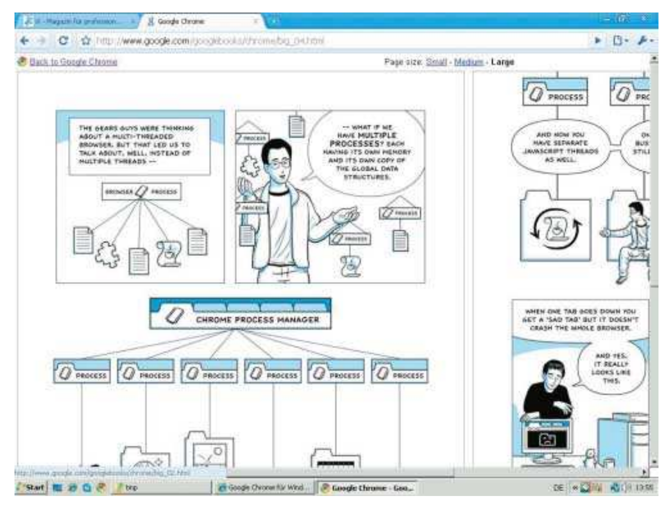
Technisch zeichnen Chrome zwei Aspekte aus: die Rolle der Tabs (Reiter) und die Javascript-Engine V8. Anders als in bisherigen Browsern sind die Tabs in der Anzeige „nach oben“ gerutscht, sie lassen sich sogar in ein anderes Fenster auslagern. Die tiefere Bedeutung dieser Anordnung liegt darin begründet, dass nicht ein Teilprozess, sondern vielmehr ein „ganzer“ Prozess jeden einzelnen Tab steuert. Das heißt zwar mehr Speicherverbrauch durch die Anzahl der Prozesse, gleichzeitig aber, dass nicht wegen eines einzigen hängenden Tab der Browser insgesamt „abstürzt“. Die Analogie zum Betriebssystem liegt auf der Hand: Wer Webanwendungen wie E-Mail oder Tabellenkalkulation nutzt, möchte nicht alles auf einmal verlieren.

V8 (code.google.com/p/v8/) heißt die von Google in Dänemark entwickelte Javascript-Engine, die den ECMA-Standard 262 in der dritten Ausgabe implementiert, wie sie die großen Browser unterstützen. V8 ist in C++ geschrieben, läuft unter Windows XP/Vista, Mac OS X und Linux-Systemen (Intels 32-Bit-Architektur und ARM). Entwickler können sie sowohl stand-alone als auch embedded verwenden.

Javascript-Code wird von der Engine in Maschinencode kompiliert und erst danach ausgeführt. Für Entwickler gibt es im Seitenmenü (links neben dem Schraubenzieher) eine Javascript-Konsole und -Fehlersuche sowie einen Task-Manager, der anzeigt, welcher Tab, welches Plug-in wie viel Speicher verbraucht. Speicherfresser kann man markieren und löschen.

Dem klassenlosen Javascript haben die Dänen für V8 versteckte Klassen verpasst, in die sie Objekte mit denselben Eigenschaften packen, damit sie optimierbar werden.

Trotz des Betastadiums sieht Chrome recht ausgereift aus, was nicht heißt, dass Google nicht noch vieles verbessern wird. Vor allem mit den Sicherheitsbedenken dürfte sich die Firma beschäftigen müssen. Google-Sprecher Kay Oberbeck hat zumindest versichert, dass es keine Verbindung zwischen der erwähnten ID und Eingaben im Suchfeld gebe. Und dass die Kalifornier die Speicherdauer von IP-Adressen von 18 auf 9 Monate heruntersetzen wollen, wäre ein gutes Zeichen, wenn der Zuständige nicht schon gesagt hätte, eine weitere Reduzierung komme nicht infrage. (hb)



Anfang September verbreitete sich die Kunde eines Comics zu Googles kommendem Browser wie das sprichwörtliche Lauffeuer.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

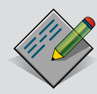
Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Projekterfolg kein Glücksspiel

Die Unternehmensberatung Roland Berger hat in einer Studie zum Scheitern von IT-Großprojekten mangelndes Risikomanagement als eine der Hauptursachen identifiziert. Neben der Analyse beschreibt die Untersuchung, wie man es besser machen kann. Bei fast 50 Prozent aller Projekte fehlt es laut Berger an einem Stab, der sich angemessen um Risikomanagement und operative Steuerung kümmert. In die Bewertung von Krisenprojekten fließen meist nur direkte Kosten ein, dabei seien die indirekten in der Regel erheblich höher. Weitere Handicaps in großen Vorhaben ergeben sich aus langer Projektdauer, häufig wechselnden Anforderungen, mangelhafter Dokumentation und steigenden Mitarbeiterzahlen. Und den eingesetzten Techniken fehlt oft die notwendige Reife.

KURZ NOTIERT



Kleinigkeiten: Mit der Release 5.1 ihrer Prozessmanagement-Suite deckt die Berliner Inubit AG BPMN 1.1 sowie WS-BPEL 2.0 ab. Zu den weiteren unterstützten Standards zählen UDDI 3.0, WS-Security und WS-Policy.

Erweitert: Signaturspezialist Authentidate hat seinen E-Billing Signature Server erweitert. Die wichtigste Neuerung: ein Regelwerk, das es erlaubt, jede Signaturkarte über Parameter (Seriennummer, Herausgeber, Besitzer et cetera) anzusprechen. Auf diesem Weg soll die Nutzung spezifischer Signaturkarten für bestimmte Rechnungen möglich sein.

Ausgebaut: Die Dortmunder E-Spirit AG erweitert ihre Content Management Suite Firstspirit um Exaleads Intranet-Suchmaschine one:enterprise. Durch die Kopplung der Personalisierungsmodelle beider Programme lassen sich geschützte Dokumente und Seiten durchsuchen. Der Benutzer sieht nur die Treffer, die er laut Berechtigungsstufe sehen darf.

Zertifiziert: Die Prozessmanagementplattform Aris der IDS Scheer erhält die TOGAF-Zertifizierung (The Open Group Architecture Framework). Die Spezifikation dient dem Entwurf, der Planung, Implementierung und Wartung von IT-Architekturen. Für nichtkommerzielle Zwecke bietet die Open Group das Rahmenwerk kostenfrei an. Insbesondere bei Behörden entwickelt es sich zur Standardmethode.

Mehr Austausch: Sage Software bringt die Classic Line 2009 auf den Markt. Beispielsweise beherrscht die ERP-Software für kleine Unternehmen den elektronischen Dokumentenaustausch, die digitale Signatur und Überweisungen im SEPA-Format. Sowohl die Standard- als auch die Professional-Version ist webfähig, eine lokale Installation des Pakets ist nicht mehr erforderlich.

Mehr Zukunft: Embarcadero hat die 2009er-Versionen von Delphi und C++ vorgestellt. Der C++ Builder soll bereits den kommenden Standard C++0x unterstützen. Eine sogenannte Datasnap-Architektur hilft dem Programmierer bei der Entwicklung von Datenbankanwendungen. Die Architect-Editionen der Werkzeuge enthalten das Datenmodellierungs-Tool ER/Studio. Beide IDEs beherrschen Unicode.

Eingebettet: Gemeinsam entwickeln MID und oose eine SysML/UML-Modellierungsmethode für eingebettete Systeme. Entstehen soll ein Rahmenwerk aus Entwicklungsprozess, Modellierungstechniken und Werkzeugkonfigurationen. Grundlage für die Methode namens M3EE sind MIDs Innovator und das Open-Source-Generatorframework oAW (openArchitectureWare).

Kurzes Gastspiel für Dynamics Entrepreneur

Überraschend verkündete Microsoft Ende August, dass Dynamics Entrepreneur, die hauseigene Unternehmenssoftware für kleine Unternehmen, zum 1. September 2009 aus den Preislisten verschwindet. Stattdessen soll die kommende Version des „großen“ Dynamics NAV 2009 einen speziellen Client für diese Firmen enthalten. Verharmlosend nennt es die Pressemitteilung eine „Optimierung der Produktpalette für kleine und mittelständische Unternehmen“.

Anwendern des Entrepreneur-Systems verspricht der Hersteller immerhin, dass sie entsprechende neue Lizenzen kostenlos erhalten und unter Mitnahme des gesamten Datenbestandes wechseln können. Service will man bis Februar 2013 leisten. Das abgespeckte Dynamics NAV, das zu Jahresbeginn auf den Markt kam, beschrieb Microsoft als „integrierte, einfach zu bedienende Unternehmenssoftware für wachstumsorientierte Kleinunternehmen“. Die ERP-Software war für maximal fünf gleichzeitig aktive Clients ausgelegt und bot ein paar Anpassungsoptionen. Offenbar vermissten die Anwender jedoch Flexibilität und Branchenfunktionen.

Bei Dynamics NAV steht ein durchgreifender Architekturwechsel auf eine dreistufige Systemarchitektur an. Über ein Rollenkonzept sollen auch Firmen das große Paket nutzen können, für die es eigentlich überdimensioniert ist. Microsoft wird das Angebot möglicherweise um eine Onlinevariante ergänzen. Mitte November soll die neue Version der Unternehmenssoftware vorgestellt werden. Der Verkauf erfolgt wieder über traditionelle Vertriebspartner und nicht wie im Fall von Entrepreneur exklusiv über Actebis Peacock.

Lieferantenmanagement im SAP-Betrieb

Die Selected Services GmbH erweitert das gehostete Lieferantenportal Pool4Tool um ein Enterprise Service Repository (ESR) sowie einen Enterprise Process Monitor (EPM). Das ESR fungiert als Schnittstelle für den Transfer von SAP-Daten in das Portal. Dabei setzt man auf Standards wie SOAP und Ajax. Der EPM, der auf der SAP-eigenen Kommunikations-API iDoc basiert, soll die zwischen Pool4Tool und dem SAP-System laufenden Geschäftsprozesse überwachen. Das Portal enthält vorgefertigte Prozesse, etwa zum Erstellen von Lagerbeständen, Wareneingangsbelegen oder Rechnungen.

RFID-Projekte: Nachfrage steigt

IT-Hersteller konnten 2008 mehr RFID-Projekte realisieren als im Vorjahr. 46 % ihrer Kunden haben RFID-Systeme im Einsatz (2007: 34 %), entweder im Pilotstadium oder im Produktionsbetrieb. Zu diesem Ergebnis kommt eine Befragung von 155 IT-Unternehmen aus den USA (85 %) und Europa (8 %), die der IT-Verband CompTIA (Computing Technology Industry Association) durchgeführt hat. Als beliebteste Einsatzbereiche nannten die Befragten das Asset Tracking (32 %), gefolgt von der Personenidentifikation (25 %), dem Einzelhandel (15 %) und geschlossenen Produktionskreisläufen (9 %).

Barbara Lange

Kollaborations-Tool von Embarcadero

ER/Studio Enterprise Portal von Embarcadero soll das verteilte Modellieren von Unternehmensdaten erleichtern. Das Portal umfasst eine Suchmaschine für Metadaten, Geschäftsregeln und Modelle und ermöglicht eine Gesamtsicht auf alle Firmeninformationen. Das Produkt enthält Werkzeuge für Datenabfrage und Berichtswesen, mit denen der Nutzer auch interne Richtlinien (Governance) und gesetzliche Vorgaben (Compliance) überwachen kann.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

KURZ NOTIERT

Geschützte Daten: Von DeviceLock stammt die Endpoint-Security-Management-Plattform, die ans Netzwerk angeschlossene USB- und andere Devices kontrolliert. Der zweite Teil des neuen Produktes gegen unautorisierten Datenabfluss im Unternehmen kommt von IronKey, Hersteller von USB-Sticks mit Datenverschlüsselung. Mit dem neuen Produkt kann man beispielsweise eine verschlüsselte Datenablage erzwingen.

E-Mail-Sicherheit: Eine neue Softwareversion des Security Gateway stellt die Karlsruher Astaro AG vor. Schwerpunkt der neuen Features ist die E-Mail-Sicherheit, etwa in Form von Verschlüsselung. Neu sind auch ein Active Directory Browser sowie die Überarbeitung des Benutzerportals für die Verwaltung der E-Mails und VPN-Verbindungen.

Rootkit-Historie: Um Rootkits geht es in der jüngsten Analyse des Virenschutzherstellers Kaspersky. In ihr erläutert die Virenanalystin Alisa Shevchenko die Funktionsweise von Stealth-Techniken, ihre Entwicklung und Historie sowie aktuelle Trends. Der mehrseitige Artikel ist auf der Kaspersky-Website (s. *iX*-Link) zu finden.

Sicherheits-Appliance: Auf kleine Netzwerke ist die neue Appliance LiSS 700 aus dem Hause Telco Tech ausgerichtet. Das mit 4-Port-Switch ausgestattete Gerät übernimmt Router-, Bridge- und PPP-Funktionen und kann zum Beispiel externe Mitarbeiter via Internet mit dem Firmennetzwerk verbinden. VPN-Funktion, Paketfilter und Intrusion Detection sollen Angreifer fernhalten und Datenmanipulation oder -klau ausschließen.

iX-Link ix0810021

Zeiterfassung und Zutritt via Iriserkennung

Iriserkennung wird bislang überwiegend im Hochsicherheitsbereich eingesetzt. Mit der neuen Produktlinie ByoAccess, die im niedrigeren Preissegment angesiedelt ist, will der Hersteller Byometric systems AG (www.byometric.com) auch kleinen und mittleren Unternehmen die Nutzung dieses biometrischen Verfahrens eröffnen.

Im Unterschied zu anderen Systemen nutzt ByoAccess einen Iriserkennungs-Controller namens „ByoAcces multi“ (siehe Bild), der bis zu fünf Kameras an verschiedenen Türen steuert. Die Software „ByoAccess time“ kombiniert das Zutrittskontrollsystem mit den Zeiterfassungssystemen des Unternehmens. Geplant ist eine Vorstellung des Systems Anfang Oktober auf der Fachmesse „Security Essen 2008“.




Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Haftung von Suchmaschinen- und Wiki-Betreibern

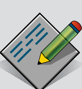
Das Oberlandesgericht Nürnberg hat in den Streit um die Verantwortung für Webinhalte von Suchmaschinenbetreibern eingegriffen. In ihrem Beschluss (Az. 3 W 1128/08) differenzierten die Richter zwischen der Haftung vor einer Abmahnung durch Dritte wegen rechtswidriger Inhalte auf den von ihren Suchmaschinen indexierten und verlinkten Seiten und der Haftung nach Zugang einer diesbezüglichen Abmahnung oder eines anderen Hinweises auf das Vorhandensein solcher Inhalte.

Ein Suchmaschinenbetreiber ist vor einer Abmahnung, also bevor er die für die Haftung nach dem Telemediengesetz so wichtige „Kenntnis“ erlangt hat, kein Störer und damit nicht für Webinhalte verantwortlich, auf die er verlinkt. Das ändert sich nach Auffassung der Richter erst, wenn er einen Hinweis auf die Inhalte erlangt und eine Prüfung durch ihn dann eindeutige und klare Rechtsverletzungen ergibt. Das bedeutet, ihm wird nicht abverlangt, schwierige – weil nicht eindeutige – Sachverhalte juristisch zu prüfen oder gar externe Juristen einzuschalten.

So sieht es auch das Oberlandesgericht Nürnberg (Az. 3 W 1128/08). Sobald aber eine entsprechende Abmahnung eingeht, ist „einem der weltweit größten Suchmaschinenbetreiber im Einzelfall zuzumuten, in eine Überprüfung der Abmahnung einzutreten“. Ergibt eine juristische Prüfung dann eine Rechtsverletzung, muss der Suchmaschinenbetreiber den Webinhalt sperren. Andernfalls kann er selbst in die Haftung genommen werden.

Ein Urteil des Landgerichts Köln (Az. 28 O 344/07) hat zur Haftung von Wikipedia Stellung genommen. Da Wikipedia als Betreiber der Plattform sich deren Inhalte „nicht zu eigen macht“, können die Wikipedia-Verantwortlichen ebenso wenig als Störer in Anspruch genommen werden wie der Admin-C der Plattform, für den dies nach Auffassung der Richter sogar noch ferner liegt. Dazu im Widerspruch steht eine Entscheidung des Amtsgerichts Hamburg (Az. 36A C 124/07), die das Oberlandesgericht Hamburg bestätigte. Demzufolge haftet der Betreiber eines Wiki, in das Dritte online Beiträge einstellen können, für dessen rechtswidrige Inhalte. In diesem Fall ging es um Persönlichkeitsrechte eines Rechtsanwalts. *Tobias Haar*

KURZ NOTIERT



Compliance-Unterstützung: In seinem neuen Compliance Guide für Open-Source-Software erläutert das Software Freedom Center den richtigen Umgang mit dieser Software. Er ist abrufbar unter www.softwarefreedom.org

Keine Kündigung per SMS: Das Landesarbeitsgericht Hamm (Az. 10 Sa 512/07) sieht darin einen Verstoß gegen die erforderliche Schriftform. Auch ein Auflösungsvertrag kann nicht per SMS zustande kommen.

Datenschutzpflicht: Ein neues US-Gesetz verlangt, dass Unternehmen Identitätsdiebstählen aktiv vorbeugen müssen. Die Vorschriften treten am 1. November in Kraft und betreffen auch ausländische Unternehmen, die geschäftlich in den USA tätig sind.

Keine Sperrung des Internetzugangs: Die deutsche Filmindustrie will die Internetanbieter für einen „deutschen Weg“ bei der Verfolgung von Raubkopien gewinnen. Anders als in Frankreich soll es aber nur Abmahnungen geben.

Widerspruchsrecht gegen Melderegisterauskünfte: Bundesdatenschützer Schaar will dem Missbrauch durch Unternehmen, die diese Daten sammeln, Einhalt gebieten. Weitgehend unbekannt ist, dass Meldeämter auch ohne „berechtigtes Interesse“ Personenauskünfte erteilen.

Chinesische Regierung will geistiges Eigentum stärken

Noch vor den Olympischen Spielen hatte die chinesische Regierung eine neue „Intellectual-Property“-Strategie vorgestellt. Sie beabsichtigt Maßnahmen zu ergreifen, um Rechte des geistigen Eigentums wie Patente, Urheberrechte et cetera besser durchsetzen zu können. Ausdrücklich war davon die Rede, dass die gesetzlichen Rahmenbedingungen für geistige Schutzrechte „verbessert werden müssen“.

Auch die Durchsetzung von Schutzrechten und deren Registrierung müssen „gestärkt“ werden, heißt es in der offiziellen Verlautbarung der chinesischen Regierung. Daneben wolle man die Rechtsdurchsetzung billiger, die Rechtsverletzung aber teurer machen. Insgesamt sollen in diesem Bereich faire Marktbedingungen geschaffen werden.

Bei der Umsetzung rechtlicher Rahmenbedingungen will die Regierung stärker auf Transparenz und auf die Beteiligung von Unternehmen, Unternehmensverbänden und der Öffentlichkeit am Gesetzgebungsverfahren achten. Zur Frage, ob sich spezielle Gerichte mit der Durchsetzung von Intellectual-Property-Rechten befassen sollen, soll es zunächst Studien geben.

Insgesamt lässt das Regierungsprogramm gerade für Schutzrechtsinhaber auf weitere deutliche Verbesserung im Rechtssystem Chinas hoffen. An manchen Stellen liest es sich allerdings etwas plakativ und oberflächlich.

Tobias Haar

Microsoft sperrt Produkt-Keys von gebrauchter Software

In einer Presseerklärung hat Microsoft weitere Schritte gegen die aus ihrer Sicht urheberrechtswidrige Nutzung gebrauchter Softwarelizenzen angekündigt. Nachdem das Unternehmen bei Testkäufen die Verwendung identischer Produkt-Keys bei verschiedenen Unternehmen festgestellt habe, habe man sich für diesen Schritt entschieden. Nach Auffassung der Redmonder deutet das auf Unregelmäßigkeiten bei der Übertragung von Nutzungsrechten aus Volumenlizenzverträgen hin. „Da Microsoft jedoch einer Übertragung gebrauchter Lizenzen an diese Unternehmen nicht zugestimmt hat, sind diese Lizenzen unseres Erachtens nicht wirksam übertragen worden und die Unternehmen sind nicht rechtmäßig lizenziert“, erklärt Dorothee Belz, Mitglied der Geschäftsleitung der Microsoft Deutschland GmbH. Mit der Sperrung der Produkt-Keys setze das Unternehmen nun ein klares Zeichen und schränke die Nutzung dieser Software ein.

Neben einem Hinweis auf die Webseite www.gebrauchte-software.org bietet Microsoft – unter Hinweis, dass Unwissenheit nicht vor Strafe schützt – eine kostenlose Lizenzüberprüfung über den Microsoft-Produktidentifikationsservice (kurz: PID-Service) an. Nach eigenen Angaben ergaben 96% aller Überprüfungen im Rahmen dieses Service in den letzten Jahren illegale Kopien von Microsoft-Produkten. Ob allerdings die Rechtsauffassung von Microsoft und anderen, beispielsweise Oracle, zutrifft, dass Volumenlizenzverträge (ganz oder teilweise) nur mit Zustimmung des Rechtsinhabers auf Dritte übertragen werden dürfen, bedarf nach wie vor der höchstrichterlichen Entscheidung durch den Bundesgerichtshof.

In einer weiteren Presseerklärung appellierte Microsoft an Unternehmen, ihre gebrauchten Softwarelizenzen nur bei Händlern zu beziehen, die mit dem jeweiligen Hersteller zusammen arbeiten. Branchenkennern ist klar, dass sich das Unternehmen damit gegen alle Gebrauchtsoftwarehändler, im Besonderen aber gegen usedSoft wendet, mit dem sich Microsoft sowie Oracle in Rechtsstreitigkeiten über die Zulässigkeit des Vertriebs von Gebrauchtsoftware ohne Zustimmung des Herstellers befindet.

Tobias Haar

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Echtzeitvisualisierung von Städten

Bitmanagement Software hat auf der Siggraph BS Contact Geo präsentiert. Die speziell für digitale Inhalte aus Geo-Informationssystemen konzipierte Visualisierungssoftware kann automatisch generierte 3D-Daten einlesen und wiedergeben, beispielsweise 3D-Städtemodelle (s. Abb.). Für die qualitativ hochwertige Darstellung großer Datensätze im Internet unterstützt die Software die ISO-Standards VMRL sowie den XML-basierten Nachfolger X3D, die X3D-Earth Initiative, das vom Khronos Konsortium definierte XML-Schema (XSD) Collada 1.5.0 als Austauschformat für 3D-Inhalte sowie weitere geo-relevante Features wie GeoCodierung und GeoMapping von Texturen.

Der Viewer stellt den Unternehmensangaben zufolge die Inhalte von GIS-Anwendungen in Echtzeit auf dem PC des Endbenutzers dar. Das Rendering der Daten erfolgt nicht vorab auf Servern der Anbieter. Durch die Echtzeitfähigkeit sind interaktive Nutzungskonzepte denkbar. Die Anwender sollen so neue Freiheiten für die Navigation durch Inhalte beziehungsweise bei der Begehung einer Umgebung erhalten. In die Anwendung eingebaute Softwaresensoren erkennen an den modellierten Objekten, ob und welche Interaktionen damit möglich sind. Damit erweitert sich der Interaktionsradius der Anwender mit den Objekten. Sie können etwa Türen öffnen und einen Rundgang durch mehrere Räume machen.

Ein weiterer Vorteil der Modellierung im Vergleich zum Film ist die Tatsache, dass infolge der Berechnung des Contents auf dem Client die zu übertragenden Datenmengen so weit reduziert werden, dass sie beim Download oder Streaming im Internet kaum noch ins Gewicht fallen. Die optimierte Speicherverwaltung durch preemptives Caching soll die Performance zusätzlich verbessern. Der Hersteller bietet die Visualisierungskomponenten zu Testzwecken ohne Funktionsbeschränkungen zum Download an (www.bitmanagement.com). (*Susanne Franke*)

iX-Link ix0810025



Neuer Standard für 3D-Daten

Die von Bonner Forschern in Zusammenarbeit mit SIG3D der Geodateninfrastruktur NRW entwickelte City Geography Markup Language (CityGML) soll als neuer Standard die Darstellung, die Speicherung und den Austausch der 3D-Daten von Stadt- und Landschaftsmodellen vereinheitlichen. CityGML ist eine Anwendung des Encoding Standards GML3 (OpenGIS Geography Markup Language 3), den das Open Geospatial Consortium (OGC) und die ISO als internationalen Standard anerkennen (siehe *iX*-Link). Das XML-Schema legt genau fest, wie ein 3D-Modell zu beschreiben ist, sodass sich aus diesen Angaben die Darstellung rekonstruieren lässt. Das OGC hat die Version 1.0.0 von CityGML als offiziellen OGC-Standard akzeptiert. Neben Stadtplanung und Architekturdesign gelten unter anderem die Umwelt betreffende Simulationen oder Katastrophenhilfe als Anwendungsgebiete für den Austausch raumbezogener Städtedaten.

iX-Link ix0810025

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Renesas stellt Dual-Core-CPU SH7786 vor

Für Multimediageräte, 3D-Navigationssysteme und anspruchsvolle Automotive-Applikationen hat Renesas (eu.renesas.com) den Dual-Core-Prozessor SH7786 entwickelt. Die im 65-nm-Prozess gefertigte CPU enthält zwei 32-Bit-Kerne (SH-4A von Hitachi), die mit maximal 533 MHz arbeiten und symmetrisches sowie asymmetrisches Multiprocessing (SMP/AMP) beherrschen. Der integrierte Memory-Controller unterstützt 32 Bit breites DDR3-SDRAM (533 MHz). Eine Display Unit bedient LCD-Panels bis zu einer Auflösung von 854×480 Pixeln.

Erweiterungen lassen sich an den PCI-Express-Bus anschließen, der 4+1 oder 2+1+1 Lanes bereitstellen kann, oder an zwei I^2C-Schnittstellen. Außerdem sind ein Fast-Ethernet-Port und zwei USB-2.0-Anschlüsse integriert, von denen sich einer wahlweise als Host- oder Geräteport konfigurieren lässt.

Um die Entwicklung neuer Systeme auf Basis des SH7786 zu beschleunigen, kooperiert Renesas mit dem Betriebssystem-Anbieter QNX (www.qnx.com) bei der Erweiterung des Realtime-OS QNX Neutrino sowie der Eclipse-basierten Entwicklungsumgebung Momentics Tool Suite. Beide eignen sich gut für den Renesas-Prozessor, weil sie sowohl symmetrisches als auch asymmetrisches Multiprocessing unterstützen.

Multi-Core-Prozessoren und -Betriebsysteme gewinnen im Embedded-Umfeld an Bedeutung. Die vorherrschende Tendenz, immer mehr Funktionen in einem Gerät unterzubringen, geht mit einem Ruf nach mehr Rechenleistung einher, die sich bei gleichzeitig geringer Wärmeabgabe ausschließlich mit Mehrkern-Prozessoren realisieren lässt. *Axel Urbanski*



Via kündigt Nano-ITX-Board mit VX800 an

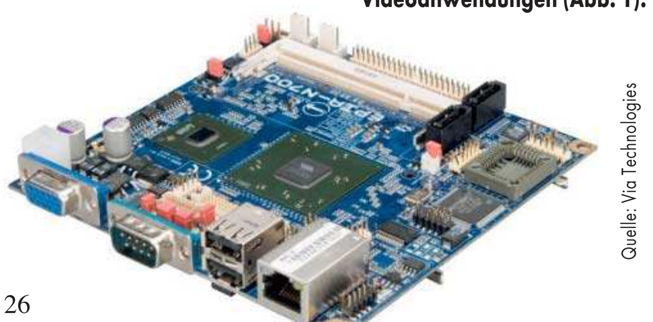
Auf die geringen Abmessungen von nur $12 \times 12\ cm^2$ bezieht sich die Bezeichnung Nano-ITX bei Vias neuem EPIA N700. Das Board ist in zwei Varianten erhältlich: mit der 500 MHz schnellen Stromspar-CPU Eden oder dem höher getakteten C7-Prozessor (1,5 GHz). Der einzige Speichersockel unterstützt bis zu 2 GByte DDR2-SDRAM.

Außerdem enthält das N700 den von Via „Media System Processor“ genannten VX800-Chipsatz. Er enthält die North- und Southbridge sowie den DirectX-9-kompatiblen Grafikbeschleuniger „Chrome 9“ für 2D und 3D, der auch beim Dekodieren der Videoformate MPEG-2, MPEG-4, WMV9, VC1 und DivX hilft.

Zusätzlich zum VGA-Anschluss an der Rückseite bietet das N700 ein LVDS-Interface (Low Voltage Differential Signalling) für ein TFT-Panel. Außerdem stehen vier USB-2.0-Ports (zwei intern), Gigabit-Ethernet, drei interne und eine externe serielle Schnittstelle zur Verfügung. Ein ATA- und zwei SATA-2-Ports erlauben den Anschluss gängiger Festplatten und optischer Laufwerke. *Axel Urbanski*



Vias Nano-ITX-Board EPIA N700 enthält neben einer Eden- oder C7-CPU einen VX800-Koprozessor für Grafik- und Videoanwendungen (Abb. 1).



Quelle: Via Technologies

Hardware-Debugger für Multi-Core-Systeme

Für Entwickler von Mehrkern-Systemen hat Wind River (www.windriver.com) den Hardware-Emulator ICE 2 entwickelt. Er eignet sich für 32- und 64-Bit-Systeme sowie System-on-a-Chip-Lösungen (SoC) mit 1 bis 16 Prozessorkernen und nutzt die JTAG-Methoden (Joint Test Action Group) nach dem IEEE-Standard 1149.1. Das erlaubt es dem Entwickler, der Originalschaltung bei der Arbeit zuzusehen, was wiederum das Testen und Debuggen erleichtert. Dazu muss er sich nicht wie sonst üblich im selben Raum befinden: Gerät und Zielsystem lassen sich über die integrierte Ethernet-Schnittstelle fernsteuern.

Nach Angaben des Herstellers fügt sich ICE 2 nahtlos in die Eclipse-basierte Wind River Workbench ein. Die Entwicklungsplattform lässt sich sowohl für VxWorks und Wind River Linux als auch für generisches Linux (ab Kernel-Version 2.4.26) sowie für Express Logics Echtzeit-Betriebssystem ThreadX nutzen. Auf dem Host kann neben diversen Linux-Varianten von Red Hat und Suse auch Solaris/Sparc, Windows XP SP2 oder Vista zum Einsatz kommen.

Zurzeit ist das Gerät für Multi-Core-Prozessoren wie den MIPS64-Ableger Octeon von Cavium (www.cavium.com) und Power-basierte CPUs von Freescale (www.freescale.com) geeignet, etwa die Modelle MPC55xx, MPC 8572, MPC8640 und MPC 8641D. Außerdem hat der Hersteller Unterstützung für Freescales SoC-Plattform QorIQ angekündigt. *Axel Urbanski*



Quelle: Wind River

Wind Rivers ICE 2 erlaubt die Fehlersuche in Mehrkern-Embedded-Systemen sogar aus der Ferne (Abb. 2).

Wind River übernimmt Linux-Firma Mizi

Für 16 Millionen US-Dollar in bar sollen die freien Anteile des südkoreanischen Unternehmens Mizi Research bis zum 31. Oktober in den Besitz des US-Unternehmens Wind River übergehen. Beide Unternehmen haben eine entsprechende Vereinbarung unterzeichnet.

Mizi (www.mizi.com) wurde 1999 gegründet und beschäftigt 65 Mitarbeiter; die Unternehmensanteile befinden sich zurzeit im Privatbesitz. Software des Unternehmens findet sich in über 20 elektronischen Konsumerprodukten wieder. Die Entwicklungsplattform Prizm – ein SDK für Telefone, PDAs, Automotive-Applikationen und mobile Unterhaltungselektronik – kommt unter anderem bei Samsung Electronics, LG Electronics und Renault Motors zum Einsatz.

Wind River (www.windriver.com) liefert Services, Entwicklungstools sowie Betriebssysteme für den Embedded-Bereich. Neben dem Real-Time-Betriebssystem VxWorks gehören verschiedene Linux-Varianten, darunter ein RT-Linux und ein Automotive-Linux, zum Angebot. Mit der in Seoul ansässigen Softwareschmiede Mizi will das Unternehmen seine Position im Embedded-Linux-Markt bei mobilen Geräten verstärken. *Axel Urbanski*



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Webemulator für mehr als 1600 mobile Endgeräte

Entwickler von Webanwendungen für mobile Endgeräte haben mit einer Unzahl unterschiedlicher Browser, Features und Bildschirmauflösungen zu kämpfen. Keynote Systems, Insidern bekannt durch Performance- und Verfügbarkeitsmessungen von Websites, bietet nun mit dem Mobile Interactive Testing Environment (MITE) ein Produkt, das über 1600 Endgeräte von mehr als 60 Herstellern emulieren können soll. Die Bibliothek der Endgeräte ist durch eigene Definitionen erweiterbar und lässt sich über einen Update-Dienst aktualisieren.

Getestet werden können beliebige Webseiten, geladen entweder direkt über eine bestehende Internetverbindung oder über die eines mobilen Endgeräts. Im letzteren Fall sind zur Simulation einer echten mobilen Verbindung länderspezifische WAP-Anbieter wählbar.

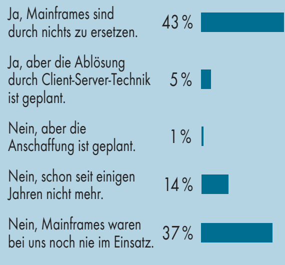
Im Emulator selbst kann der Entwickler nach Belieben Webseiten laden. Die Emulationsumgebung speichert neben den technischen Details der Verbindung wie Header, Datenmenge und Geschwindigkeit detaillierte Informationen zu den Medien der einzelnen Seiten. Das System macht darauf aufmerksam, wenn Bilder die Display-Dimensionen sprengen oder das Endgerät Stylesheets nicht darstellen kann. Neben der Möglichkeit, Quellcodes der Seiten und Stylesheets direkt anzuzeigen, lassen sich heruntergeladene Klingeltöne direkt in der Software abspielen. Sessions können gespeichert und per Skript wiederholt werden.

Das Mobile Interactive Testing Environment ist nach Registrierung über die Homepage von Keynote Systems als 15 Tage lauffähige Trial-Version herunterzuladen; eine Lizenz kostet 1500 US-$ pro Jahr inklusive Updates der Endgerätedatenbank.

Marcus Proest

iX-Umfrage: Big Iron lebt

Nach den Ergebnissen der Online-Umfrage, die parallel zu *iX* 9/07 auf www.ix.de lief, sind Mainframes nach wie vor angesagt. Satte 43 % fanden, der Mainframe sei unersetzlich. Deutlich weniger, nämlich 19 %, wollen ihre Großrechner abschaffen oder haben dies bereits getan. Die genauen Ergebnisse sind der Grafik zu entnehmen.



Die nächste Umfrage startet am 17. September und dreht sich um Googles Webbrowser Chrome.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

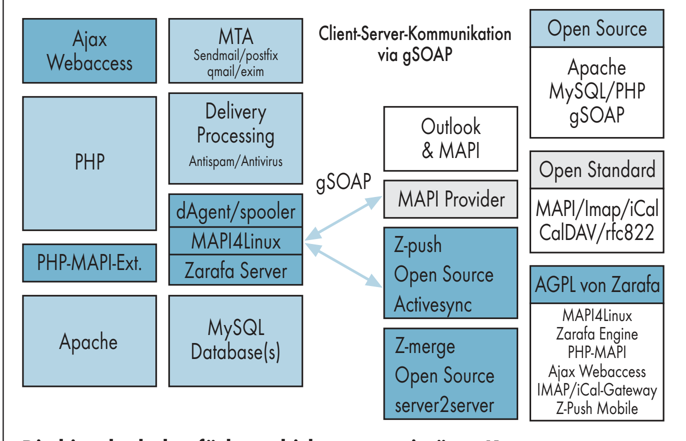
Anzeige

Zarafa wird Open Source

In der Vergangenheit musste sich die deutsch/niederländische Firma Zarafa (www.zarafaserver.de) Kritik anhören, da sie in ihrer gleichnamigen Groupware Open-Source-Komponenten wie MySQL, PHP, Apache oder gSOAP mit proprietären Teilen kombinierten. Im Oktober vergangenen Jahres gab man mit Z-Push eine Active-Sync-Implementierung unter der GPL frei, mit Erscheinen dieser Ausgabe folgt nun ein großer Schritt: Zarafa gibt bis auf den MAPI-Provider für Outlook alle bislang nicht offenen Teile unter der AGPL (Gnu Affero General Public License) frei. Bei der AGPL handelt es sich quasi um die Netzwerkvariante der GPL, die unter anderem auch Nutzern via SaaS ein Recht auf Bereitstellung des Quellcode einräumt.

Zu den jetzt freigegebenen Teilen gehören neben dem Zarafa-Server mit MAPI4Linux unter anderem eine PHP-MAPI-Erweiterung, der Ajax-Client sowie Z-Merge für die Echtzeitkoppelung mehrerer Server (siehe Grafik). Der MAPI-Provider für Outlook ist in der Download-Version auf drei Benutzer beschränkt. Wer mehr benötigt, kann zu einer der über ein Subskriptionsmodell angebotenen Business-Pakete greifen. Diese werden zum anderen auch im professionellen Umfeld benötigte Eigenschaften wie Clustering, Monitoring oder erweiterte Backup-Funktionen bieten. Darüber hinaus sollen Service- und Supportangebote für Wiederverkäufer weitere Einnahmen bringen.

Ebenfalls mit Erscheinen dieser Ausgabe soll das Projekt OpenMAPI (www.openmapi.org) an den Start gehen. Es will die MAPI-bezogenen Open-Source-Beiträge von Firmen bündeln und koordinieren – beispielsweise die Entwicklung einer freien Blackberry-Anbindung. Zum Start werden Topalis, Vipcom, Wilken und natürlich Zarafa dabei sein.



Die hier dunkel gefärbten, bislang proprietären Komponenten stellt Zarafa jetzt unter die AGPL.

KURZ NOTIERT

Update: Univention (www.univention.de) hat seinen Corporate Server UCS überarbeitet. Die neue, jetzt auch für x86_64-Systeme verfügbare Version 2.1 bietet unter anderem einen Kernel 2.6.24, ein integriertes Netzwerk-Backup (Bacula), die revisionssichere Protokollierung von Systemänderungen, eine vereinfachte AD-Integration und die verbesserte Unterstützung mobiler Endgeräte in der Groupware.

Community-Treffen: Vom 17. bis 19. Oktober kommt die deutschsprachige Ubuntu-Community zur Ubucon 08 (ubucon.de) an der Georg-August-Universität in Göttingen zusammen. Das Programm mit seiner Mischung aus Diskussionsforen, Vorträgen und Workshops soll den Austausch zwischen Anwendern und Entwicklern fördern.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

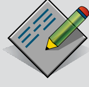
Virtuelle und physische Ressourcen im Blick

HP hat das Programmpaket Business Service Management (BSM) um Komponenten für das Überwachen und Steuern virtueller und physischer IT-Ressourcen erweitert. Der Performance Agent in der Version 4.7 kontrolliert mit nur einem Agenten pro physischem Server sowohl die reale als auch alle darauf laufenden virtuellen Maschinen nahezu in Echtzeit. Er unterstützt VMware ESX Server, AIX LPAR, Solaris Zones und HP Integrity VM. Als Vorteile der Beschränkung auf einen Agenten nennt HP eine präzisere Korrelation der Informationen sowie eine geringere Systembelastung. Ähnliches gilt für die Monitoring-Lösung Sitescope, die virtuelle und physische Systeme per Fernabfrage der Performance-Metriken überwacht. Die aktuelle Version 9.0 verfügt über einen Monitor speziell für VMware ESX. Voraussichtlich im Oktober wird zudem HPs Netzmanagement-Lösung Network Node Manager (NNM) mit neuen Funktionen für virtuelle Netzwerke verfügbar sein.

Licht in die Konfiguration bringen

Solarwinds bringt die Version 5 des Orion Network Configuration Manager (NCM, bisher unter dem Namen Cirrus vermarktet). Er unterstützt Administratoren dabei, den Zustand von Netzwerkkomponenten zu überwachen und Performance-Kenndaten zu erheben. Orion NCM v5, das auf einer agentenlosen Architektur basiert, beobachtet kontinuierlich die Gerätekonfigurationen und meldet automatisch die Verletzung vorgegebener Regeln. Die Informationen stehen über die eingebauten Syslog- und SNMP-Trap-Server zur Verfügung. Die Integration des Orion Network Performance Monitor (NPM) soll eine einheitliche Sicht gewährleisten, anhand derer die ITler Leistungsmetriken und Konfigurationsänderungen miteinander abgleichen und einen vollständigen Überblick über den Zustand der Netzelemente erhalten sollen. Zu den neuerdings unterstützten Systemen gehören unter anderem Riverbeds Steelhead, Ciscos VPN Concentrators und Dells Powerconnect Switches.

KURZ NOTIERT



Schutzherrschaft: Die Unternehmensberatung Exagon hat mit Patronage ein Werkzeug zur Optimierung von IT-Prozessen entwickelt. Der inhaltliche Kern der Software, die auf dem Scorecard-Ansatz basiert, besteht aus Referenzmodellen für die IT-bezogenen Prozesse. Diese Modell-Entwürfe definieren Ziele für die Organisation sowie Analysen und Tests aktueller Abläufe samt ihrer Kontrollen. Verfügbar sind unter anderem Referenzmodelle zu ITIL (IT Infrastructure Library) oder ISO/IEC 20000.

Eingebunden: Die Realtech AG bietet mit dem Integrationsmodul JMX-2-SMC des TheGuard Service Management Center die agentenlose Überwachung von Java-Applikationen. Es greift auf Informationen zurück, die über sogenannte MBeans bereitstehen. Die Werte sind über die standardisierte Java Management Extension (JMX) verfügbar und werden von JMX-2-SMC zentral ohne zusätzliche Software-Agenten eingesammelt.

Eingekauft: Datenbank-Krösus Oracle ging wieder einmal auf Einkaufstour. Diesmal traf es Clearapp. Die US-Firma bietet Software an, die automatisch die Komponenten einer sogenannten Composite Application sowie deren Abhängigkeiten erkennt und im Anschluss die Leistung überwacht. Mit Auptyma und Moniforce hatte Oracle bereits zuvor kleinere Spezialfirmen für Lösungen zur Performance-Überwachung übernommen.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

KURZ NOTIERT

Noch ungewiss: Der britische Anbieter von Sicherheitssoftware Sophos will für 217 Mio. € den hiesigen Konkurrenten Utimaco Safeware übernehmen. Das Einverständnis des Großaktionärs Investcorp Technology Partners besitzt man bereits. Noch ungeklärt ist die Frage, ob das Bundesministerium für Wirtschaft und Technologie den Übernahmeplänen zustimmt.

Losgelöst: Hewlett-Packard verleibt sich Colubris Networks ein. Die Produkte des Anbieters von Switchen für WLANs sollen dem HP-Bereich Procurve zugeschlagen werden.

Aufkauf: Open Text, Anbieter von Enterprise-Content-Managementsoftware, beabsichtigt Captaris zu übernehmen. Die Kapitaleigner erhalten von Captaris insgesamt rund 131 Mio. $ für ihre Papiere. Der Kauf soll bis Ende 2008 abgeschlossen sein.

Einkauf: JDA Software beabsichtigt für 346 Mio. $ den US-Konkurrenten i2 zu übernehmen. Bereits vor zwei Jahren hatte man sich mit Manugistics einen Wettbewerber für 211 Mio. $ einverleibt. Nach Gartner-Berechnungen wäre das neue Unternehmen mit einem kombinierten Umsatz von 635 Mio. $ die Nummer 3 im Markt der SCM-Software.

Kleine Schritte: Nachdem es mit Yahoo nicht geklappt hat, unternimmt Microsoft nun vergleichweise kleine Schritte und kauft für 486 Mio. $ die US-Firma Greenfield Online. Allerdings hegt man allein Interesse an der Tochtergesellschaft Ciao, die in Europa Einkaufsinformations-Portale betreibt. Diese Plattformen will man in MSN Live Search integrieren. Ciaos Konzernmutter Greenfield Online steht wieder zum Verkauf.

Indiens Boom im IT-Service-Markt

Globale Verschiebung

Achim Born

Die US-Beratungsfirma Gartner erwartet, dass die künftigen Schwergewichte im IT-Dienstleistungsmarkt aus Indien stammen. Um den etablierten US-Größen bei Großaufträgen tatsächlich den Rang abzulaufen, müssten sie allerdings enger mit Anwendern zusammenarbeiten und weltweit präsent sein.

Spätestens in drei Jahren soll es so weit sein. Einer Gartner-Untersuchung zufolge sollen die drei führenden indischen IT-Dienstleister 2011 den bislang dominierenden US-Konzernen immer öfter Großaufträge wegschnappen können. Bereits heute werden nach Beobachtung der US-Berater die indischen Firmen Tata Consultancy Services (TCS), Infosys Technologies und Wipro Technologies wiederholt zur Angebotsabgabe aufgefordert. Und zwar immer dann, wenn Konzerne größere Entwicklungs- und Outsourcing-Vorhaben planen, deren Volumen mehrere Hundert Millionen Dollar umfassen.

Noch können die indischen Unternehmen den US-Größen nur selten Großaufträge abjagen. Allein IBMs Umsätze in diesem Segment beliefen sich im vergangenen Jahr auf das Zehnfache der Einnahmen von Tata Consultancy Services, des größten indischen Anbieters. In Sachen Marktkapitalisierung fällt der Vergleich jedoch anders aus. Die drei führenden Firmen aus Indien bewegen sich schon auf dem Niveau von Accenture, obgleich der US-Konzern 2007 vier- bis fünfmal höhere Serviceeinnahmen erzielte. Ein Grund für die Wertschätzung der Börse sind die herausragenden Wachstumswerte der indischen Serviceanbieter. Sie steigern ihren Umsatz dreimal so schnell wie die etablierte US-Konkurrenz und konnten innerhalb von drei Jahren ihre Unternehmensgröße mehr als verdoppeln. Selbst als Milliarden-Dollar-Firmen können sie das Wachstumstempo beibehalten; der Vorsprung der US-Konkurrenz schwindet peu à peu.

Der im Vergleich zu den US-Konzernen deutlich geringere Pro-Kopf-Umsatz weist aber darauf hin, dass die indischen Anbieter bislang in erster Linie mit einfacheren, vergleichsweise personalintensiven Dienstleistungen betraut waren. Mittlerweile haben IBM & Co. jedoch selbst in großem Maße eigene Offshore-Kapazitäten aufgebaut. Hinzu kommt, dass die wachsenden Einkommenswünsche der indischen Fachkräfte den bisherigen Preisvorteil aufzehren.

Gartner empfiehlt den indischen Unternehmen deshalb, das bisherige Geschäftsmodell zu überarbeiten. Um tatsächlich mit den etablierten Anbietern auf Augenhöhe zu operieren, könnten sie sich nicht mehr allein darauf verlassen, höhere Einnahmen einfach über mehr Mitarbeiter zu generieren. Stattdessen sollten sie nach dem Vorbild der US-Konzerne enge Beziehungen zu den Anwendern aufbauen, um auf diesem Weg an die lukrativeren Geldtöpfe im Servicegeschäft zu gelangen.

Die Aktivitäten der führenden indischen Konzerne in jüngster Vergangenheit belegen, dass man die Analysten-Botschaften durchaus verstanden hat. Infosys übernahm beispielsweise vor wenigen Tagen für rund 510 Mio. € den britischen SAP-Dienstleister Axon, um das Geschäft in der alten Welt anzukurbeln. Wipro wiederum eröffnete im September in Köln bereits die siebte Niederlassung hierzulande und kündigte an, in der Domstadt ein weiteres Entwicklungszentrum zu etablieren. (WM)

Big Player im IT-Service-Markt

Firma	Jahr	Umsatz	Wachstum	Mitarbeiter	$ pro Kopf
TCS	2007	5,718	32,45	111407	51320
	2006	4,317	44,89	89419	48280
	2005	2,979	33,31	66480	44820
	2004	2,235		45715	48890
Infosys	2007	4,176	35,15	91187	45800
	2006	3,090	43,59	72241	42770
	2005	2,152	35,18	52715	40820
	2004	1,592		36750	43320
Wipro	2007	3,393	37,94	82122	41310
	2006	2,459	35,50	67818	36260
	2005	1,815	34,09	53742	33770
	2004	1,354		41857	32340
IBM Services	2007	54,144	12,12	368558	146910
	2006	48,291	1,86	355766	135740
	2005	47,407	2,43	329373	143930
	2004	46,283		329001	140680
Accenture	2007	22,134	4,07	170000	130200
	2006	21,268	7,65	140000	151910
	2005	19,757	-0,53	123000	160630
	2004	19,863		103000	192840
EDS	2007	21,453	17,69	139000	154340
	2006	18,228	6,63	118000	154470
	2005	17,094	13,10	119000	143650
	2004	15,114		117000	129180

Umsatzzahlen in Milliarden Dollar, Wachstum in Prozent

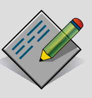
Quelle: Gartner 08/2008

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

KURZ NOTIERT



Lukrativ: Circa 5,2 Millionen Mini-Notebooks werden dieses Jahr einen Abnehmer finden. 2009 sollen es laut Prognose der Gartner Group sogar 8 und bis 2012 insgesamt 50 Millionen Geräte sein.

Erweitert: Microsoft und Novell kündigten weitere Investitionen im Rahmen ihrer Zusammenarbeit an, die die Interoperabilität von Windows- und Suses Linux Enterprise Server vertiefen soll. Microsoft verpflichtet sich, für seine Kunden bis zu 100 Mio. $ entsprechende Novell-Zertifikate zu kaufen, die sich gegen erweiterten Support des Open-Source-Lieferanten einlösen lassen. Bislang konnte Novell im Rahmen der Zusammenarbeit mit Microsoft bereits mehr als 156 Mio. $ fakturieren.

Erhöht: Der hiesige Markt für digitale Konsumelektronik soll laut Bitkom in diesem Jahr um 5,4 % auf 12,4 Mrd. € wachsen. Größter Einzelposten bleiben Flachbildfernseher, die voraussichtlich um 16 % auf gut 4,9 Mrd. € zulegen.

Servermarkt in EMEA mit guten Zuwächsen

Einnahmen durch den Verkauf von Servern legten laut IDC in Europa, Afrika und dem Nahen Osten (EMEA) im zweiten Quartal 2008 um knapp 9 % auf fast 4,5 Mrd. $ zu. Die Verkaufszahlen stiegen im betrachteten Zeitraum um 12,4 % auf fast 700 000 Systeme. Angetrieben wurde das Wachstum in erster Linie in Zentral- und Osteuropa (17,8 %). Dicht gefolgt von den Regionen Naher Osten und Afrika mit 16,1 %. Wenig überraschend fiel das Plus im westeuropäischen Markt deutlich geringer aus. Ein Plus von 6,8 % belegt jedoch auch hier eine durchaus gesunde Entwicklung.

Das Gros der verkauften Rechner (über 95 %) war wie in der Vergangenheit mit x86-Prozessoren ausgestattet. Die Einnahmen verteilten sich indes jeweils zur Hälfte auf x86- und RISC-Architekturen. Diese Umsatzverteilung dokumentiert, dass es den Herstellern von RISC-Systemen trotz rückläufiger Stückzahlen gelang, den Umsatz um 11,3 % auszubauen. Insbesondere die Anbieter von Highend-Server/Mainframes und mittleren Systemen durften sich über ein Einnahmeplus von 22,7 % beziehungsweise 12,9 % freuen.

Nutznießer dieser Entwicklung war in erster Linie IBM. Der US-Konzern hat nach IDC-Recherchen den Umsatz mit z-Mainframes um 47,3 % steigern können. Auch Fujitsu-Siemens kann sich mit den BS2000-bezogenen Einnahmen (+21,5 %) sehen lassen. Da die Geschäfte mit den anderen Rechnerarchitekturen weniger gut liefen, ist das Gesamtplus bei FSC allerdings unterdurchschnittlich ausgefallen. Unter den führenden Anbietern erzielte allein Sun einen noch geringeren Wert. Im Gegensatz dazu stieg IBM durch ein Einnahmeplus von mehr als 18 % über alle Modelle beinahe zur Nummer 1 auf: Der Abstand zur führenden HP, vor Jahresfrist noch fast 5 Prozentpunkte, schrumpfte auf 0,6 Prozentpunkte.

Top 5 der Server-Anbieter

Platz	Hersteller	Umsatz Q2/07	Marktanteil	Umsatz Q2/08	Marktanteil	Wachstum
1	HP	1,404	34,1	1,463	32,7	4,2
2	IBM	1,219	29,6	1,440	32,1	18,2
3	Sun	0,566	13,8	0,577	12,9	1,9
4	Dell	0,362	8,8	0,425	9,5	17,2
5	FSC	0,270	6,6	0,279	6,2	3,1
	andere	0,298	7,2	0,296	6,6	-0,7
	Gesamtmarkt	4,119	100	4,479	100	8,7

Umsatzzahlen in Milliarden Dollar, Marktanteile und Wachstum in Prozent

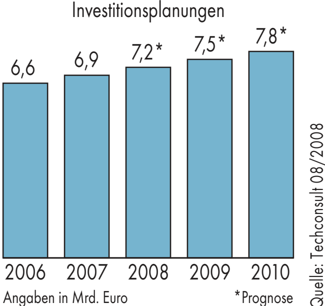
Quelle: IDC EMEA Quarterly Server Tracker, 08/2008

E-Business: Alltag für den Mittelstand

Das Internet ist heute ein fester Bestandteil der Geschäftsmodelle mittelständischer Unternehmen in Deutschland. Das zeigt die zehnte Neuauflage der Studie „E-Business im Mittelstand – IT und Innovationen für Unternehmer“, die IBM und das Wirtschaftsmagazin impulse seit 1999 alljährlich gemeinsam vorlegen. In der aktuellen Untersuchung nannten 99 % der über 1000 befragten Firmenchefs das Internet als unverzichtbar für ihr Geschäft.

Wie in der Vergangenheit führte die Mehrheit (86 %) als Motivation, E-Business-Lösungen einzuführen, den Wunsch an, neue Wettbewerbschancen nutzen zu können. An zweiter und dritter Stelle standen die Optimierung der Prozesse (77 %) und die Anforderungen der Kunden (68 %). Speziell der gehobene Mittelstand versucht den Kostendruck über den Weg der Einführung und Ausweitung von E-Business-gestützten Prozessen abzufedern. Von den Unternehmen, die mindestens einen Onlineshop realisiert haben, konnten jeweils 58 % sowohl die Organisationskosten reduzieren als auch die Produktivität steigern. 55 % erzielten Umsatzsteigerungen mit dem E-Business und 30 % konnten die Lagerkosten reduziert.

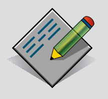
Im Unterschied zu den traditionellen E-Business-Ansätzen sind Web-2.0-Techniken in den mittelständischen Firmen noch selten vertreten. Nur 9 % der Unternehmen mit bis zu 1000 Mitarbeitern nutzen sie. Im Vordergrund stehen dabei Wikis und Blogs, die in 48 beziehungsweise 39 % dieser Firmen zum Einsatz kommen, freie Verschlagwortung setzen 17 % ein. Für die überwiegende Mehrheit (81 %) sind aber Web-2.0-Anwendungen noch nicht relevant.



Standardsoftwaremarkt weiterhin im Plus

Die gute Entwicklung des deutschen Standardsoftwaremarktes 2006 und 2007 wird sich in diesem Jahr fortsetzen. In der aktuellen Lünendonk-Studie „Führende Standardsoftware-Unternehmen in Deutschland“ prognostizieren die Befragten ein Wachstum ihres Marktsegments für 2008 von 9,8 % und für den Zeitraum 2008 bis 2013 von durchschnittlich 8,8 % pro Jahr. Die Unternehmen waren überzeugt, dass die Tendenz zu wenigen großen und vielen kleinen Softwareanbietern Bestand hat. 22 % halten das für „sehr wahrscheinlich“, 48 % für „wahrscheinlich“.

KURZ NOTIERT



Eine Nummer: Die Bundesregierung hat eine zentrale Förderberatung „Forschung und Innovation“ eingerichtet. Unter der kostenlosen Telefonnummer 08 00/26 23-009 erhalten Hochschulen, Forschungseinrichtungen und Unternehmen aus einer Hand Information zu Verfahrenswegen und Konditionen aller relevanten Förderprogramme von Bund, Ländern und der EG. Unter www.foerderinfo.bund.de sind weitere Dokumente zugänglich.

Ab in den Süden: Wer seine berufliche Laufbahn bei einem IT-Großunternehmen starten möchte, muss nach einer Meldung der PPI AG sein Glück im Süden suchen: 29 % der ausgeschriebenen Stellen für Job-Einsteiger entfallen auf den süddeutschen Freistaat, 22 % auf das „Musterländle“. Auf dem dritten Platz folgt Hessen mit 21 %.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Bei HP löst Studium die Ausbildung ab

Im Oktober kommenden Jahres bietet HP rund 115 Interessenten die Möglichkeit, ein Studium an der Berufsakademie Baden-Württemberg (BA) aufzunehmen. Das sind knapp 30 mehr als die 85 Plätze 2008. Bereits in diesem Jahr hatte HP die Plätze für BA-Studenten um 32 % gegenüber 2007 erhöht. Im Gegenzug will der IT-Konzern ab 2009 keine neuen Ausbildungsplätze für Bürokommunikation und IT-Systemkaufleute mehr anbieten. Als Grund für den Ausstieg nennt der Konzern das Ziel einer „bedarfsorientierten Ausbildung“.

Der in diesem Herbst startende Jahrgang darf seine Ausbildung noch vollenden. Danach ist es mit der beruflichen Ausbildung bei HP vorbei. Im kommenden Jahr startet zudem der neu konzipierte Studiengang „International Business Information Management“ an der Berufsakademie. Daneben werden wie bisher Studiengänge in den Bereichen Angewandte Informatik und Wirtschaftsinformatik (mit Vertiefung in IT-Servicemanagement) angeboten.

Fortbildung für arbeitslose Ingenieure

Um arbeitslose Ingenieure fit zu machen für die aktuellen Ansprüche auf dem Arbeitsmarkt, fördert das Bundesministerium für Bildung und Forschung (BMBF) Weiterbildungskurse mit 2,68 Mio. €. Die Kurse richten sich an arbeitslose Akademiker, unabhängig von der Dauer der bisherigen Erwerbstätigkeit. Die Ingenieure können sich bis zu 13 Monate an Hochschulen für den Wiedereinstieg in das Erwerbsleben qualifizieren. Die Maßnahme wird von der Otto Benecke Stiftung e. V. angeboten. Auf die Dienste der Stiftung greift das Bundesbildungsministerium seit einiger Zeit auch für das Projekt AQUA (Akademiker qualifizieren sich für den Arbeitsmarkt) zurück.

Die Fortbildungsmaßnahme wird vom BMBF und aus Mitteln des Europäischen Sozialfonds finanziert. Während der Dauer der Fortbildung beziehen die Teilnehmer weiter Arbeitslosengeld I oder II. Nähere Infos gibt es unter www.obs-ev.de. Die Zahl der offenen Stellen auf dem deutschen Ingenieurarbeitsmarkt betrug nach Recherchen des Vereins Deutscher Ingenieure (VDI) Mitte des Jahres rund 95 500 Stellen. Gleichzeitig waren 21 000 Ingenieure arbeitslos gemeldet.

Umstellung der Studienabschlüsse

Bei der Umstellung auf die Studienabschlüsse Bachelor und Master liegen in einem Ranking der Bundesländer die Stadtstaaten Berlin und Bremen vorne. In Berlin bieten zum Wintersemester 2008/2009 schon 95 % der Studiengänge die neuen Abschlüsse an. In Bremen sind es 94 %. Schlusslicht ist Bayern, wo sich mit einer Quote von 49 % viele Hochschulen wohl erst in letzter Minute von den alten Diplom- und Magisterstudiengängen trennen wollen. Das ergab eine Auswertung von Daten der Hochschulrektorenkonferenz durch den Bitkom. In den Ingenieurwissenschaften inklusive Informatik sind bundesweit bereits 82 % aller Studiengänge umgestellt. Bis 2010 müssen in den EU-Staaten flächendeckend die Abschlüsse Bachelor und Master eingeführt sein.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Zwischen Stift und Fingerkuppe

Christian Kirsch

Seit Jahren preisen Hersteller ihre Smartphones als unverzichtbares Hilfsmittel für Geschäftsleute an. Eine Exchange-Anbindung gehört mittlerweile zum Standard-Repertoire – aber was können die Geräte sonst noch?

Kamera, MP3-Player, Anbindung an Flickr und Youtube – wer die Werbung für Mobiltelefone betrachtet, könnte den Eindruck gewinnen, dass es außerhalb des Spiel- und Spaßsegments keine vernünftige Anwendung mehr gibt. Dabei übersähe er allerdings die Gruppe der relativ teuren Smartphones: Sie warten zwar ebenfalls mit Multimedia-Fähigkeiten auf, wenden sich aber in erster Linie an Geschäftsleute. Ihnen sollen sie die Arbeit unterwegs erleichtern.

An vorderster Stelle steht dabei die Anbindung an die unternehmensweite Groupware, in der Regel ein Exchange-Server. Sie soll gewährleisten, dass Mails, Termine und Kontaktdaten fern vom Büro ständig auf dem aktuellen Stand sind. Dies übernimmt meist Microsofts Activesync-Protokoll für Exchange: Es gleicht bei Bedarf die neuen Daten zwischen Handy und Server ab. Je nach Client regelt der Benutzer, wie häufig dies geschieht, über welchen Weg (WLAN, UMTS et cetera) und welche Informationen aktuell zu halten sind.

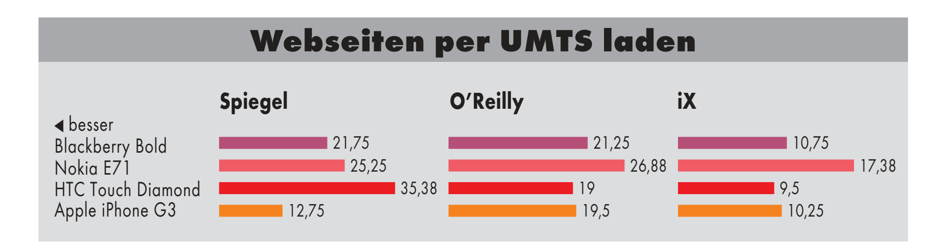
Neben diesen Ansprüchen der „always on“-Generation stehen die traditionellen Anforderungen an einen Personal Information Manager (PIM): Kontaktdaten, Termine und Aufgaben möglichst komfortabel zu verwalten. Was sich simpel und altbacken anhört, zeigt durchaus Schwächen im Detail. Mal fehlt eine brauchbare Suchfunktion, mal lassen sich keine Trennzeichen in Telefonnummern unterbringen, mal dürfen Kontaktpersonen nicht in jedem Land leben.

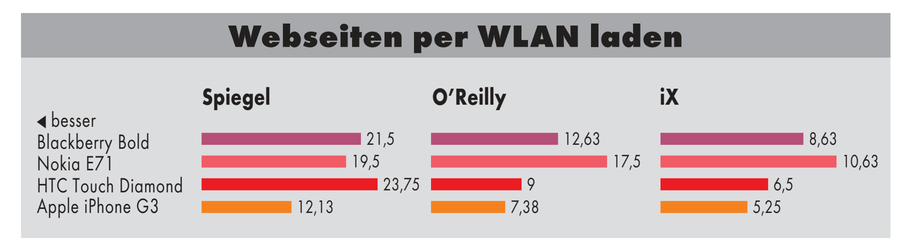
Ebenfalls aus den älteren Tagen der PDAs stammt die Desktop-Anwendung, die es auch heute noch für alle Geräte gibt – allerdings zumeist nur für Windows-Betriebssysteme. Sie soll einerseits das Sichern der Mobildaten, andererseits ihr komfortables Bearbeiten ermöglichen. Im besten Falle lassen sich damit beim Wechsel des Handys die alten Kontakte und Termine auf das neue Modell übernehmen. Wer seine Daten statt in der Desktop-Software in Outlook speichert, hat ebenfalls relativ gute Karten, sie von dort auf ein anderes Gerät zu schieben. Im Unternehmenseinsatz dürften solche individuellen Lösungen jedoch kaum eine Rolle spielen. Sinnvoll jedoch ist in jedem Fall ein lokales Backup, das alle Handydaten auf einer Speicherkarte schreiben und von dort wieder zurückspielen kann. So lassen sich Änderungen auch sichern, wenn gerade

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.





kein Internetzugang zur Verfügung steht.

Außer dem Funktionsumfang und den Fähigkeiten des Geräts spielt bei einem Alltagsbegleiter die Bedienung eine wichtige Rolle. Sind alle häufig benutzten Funktionen leicht zu finden, lässt sich das Gerät leicht an die eigenen Vorlieben anpassen, reagiert es zügig, ist die Menüführung konsistent und übersichtlich – die Antworten auf diese Fragen entscheiden darüber, ob die Arbeit mit dem Smartphone schnell und leicht von der Hand geht. Und darüber, ob sie vielleicht sogar Spaß macht.

Caching ist die Ausnahme

Im Test traten vier mit UMTS und WLAN ausgestattete Geräte gegeneinander an: der Blackberry Bold von RIM, Nokias E71, das HTC Touch Diamond und Apples iPhone 3G. Samsung war nicht bereit, sein SGH 900i als Testgerät zu stellen. Auf dem HTC-Modell lief Windows Mobile 6.1, auf dem E71 Symbian 9.x/S60, auf den anderen jeweils ein herstellereigenes Betriebssystem. Einen Exchange-Server stellte freundlicherweise 1&1 zur Verfügung.

Für den Test der Browser-Geschwindigkeit kamen drei Webseiten zum Einsatz: spiegel.de, oreilly.com und ix.de. Sie bestanden aus 146, 54 beziehungsweise 31 Dateien, die sich zu 582, 947 beziehungsweise 290 KByte Daten summierten. Diese Volumina gab Yslow an (developer.yahoo.com/yslow/). Die Webseiten lagen auf einem lokalen Webserver, was Schwankungen durch die Belastung des tatsächlichen Servers vermeiden sollte. Jede von ihnen wurde zehnmal aufgerufen, der jeweils größte und kleinste Messwert gestrichen und anschließend der Durchschnitt berechnet.

Dabei kam Überraschendes zu Tage – bis auf den Opera des HTC mochte keiner der installierten Browser die Webseiten ganz oder teilweise im Cache halten. Obwohl auf dem ausliefernden Apache ETags konfiguriert waren und er einen „Last-Modified“-Header schickte, luden das iPhone und das E71 brav die Seiten komplett. Der Blackberry speicherte alles bis auf die eigentliche HTML-Seite zwischen. Weitere Einblicke brachte die Überwachung des HTTP-Verkehrs mit *wireshark*: Während das HTC-Gerät für das wiederholte Laden der O'Reilly-Seite gut 200 TCP-Requests investierte, wandte das iPhone das Vierfache auf. Nokias E71 brachte es auf über 1800 Anfragen und benötigte doppelt so viel Zeit für das Anzeigen der Seite wie das schnellste Gerät (s. nebenstehende Benchmarks).

Bei der Anbindung via WLAN ist das iPhone der Konkurrenz überlegen, unabhängig von Caching-Fähigkeiten und Häufigkeit der Anfragen. Diesen Vorsprung büßt es jedoch bei der UMTS-Verbindung gegenüber dem HTC weitgehend ein. Das dürfte daran liegen, dass Apples Handy lediglich HSDPA mit 3,6 Mbps bietet – das HTC kann Daten doppelt so schnell laden.

Blackberry Bold

Als erste beackerte die kanadische Firma Research in Motion (RIM) das Feld der mobilen geschäftlichen E-Mail. Im Vordergrund stand bei ihr immer der Unternehmenseinsatz: RIM leitet Daten aus Exchange, Lotus und Groupwise mithilfe des Blackberry Enterprise Servers (BES) verschlüsselt an eigene Rechenzentren weiter, die sie auf die Endgeräte schicken. Dieses Konzept überzeugt einerseits viele Unternehmen, weil es keine Änderungen an ihrer Infrastruktur erfordert. Andererseits verzichten etliche Behörden und Firmen auf Blackberries, da sie Mails und sonstige Daten nicht über in anderen Ländern stehende Proxies reisen lassen wollen. Im Test stand das neueste Modell „Bold“, das erstmals UMTS und WLAN bietet (s. Abb. 1).

Nicht nur Mails sondern auch Webseiten passieren den BES, wenn man nicht den „Hotspot-Mode“ für den Browser einstellt. Dabei werden sie „angepasst“, was die Übertragungs- und Ladezeiten reduzieren soll. Das Konzept erscheint jedoch angesichts fast ubiquitärer 3G-Netze nicht mehr zeitgemäß. Zumal die Anpassung zu Fehlern führt: Bei hrs.de ist die Anzeige gefundener Hotels unbrauchbar, da der BES oder der Browser sie auf eine unsichtbare Liste zusammenschnurren lässt. Bei bahn.de konvertiert der BES die in einigen *Submit*-Knöpfen enthaltenen Umlaute in UTF-8-Sequenzen, sodass man „hinzufÃ¼gen“ lesen muss. Abhilfe schafft das Einstellen des „Hotspot-Browser“, der die Internetverbindung direkt herstellt. Trotz dieser Mängel: Der Browser auf dem Bold funktioniert deutlich besser als der des Vorgängermodells Curve, die CSS-Implementierung entspricht schon fast Desktop-Niveau.

Das zeigt sich auch beim „Blackberry“-Browser, der via BES eine ver-

iX-TRACT

- Mittlerweile gehören UMTS und WLAN ebenso zur Standardausstattung von Business-Handys wie Mail-Clients für Exchange, IMAP und POP3.
- Obwohl E-Mail die wichtigste Anwendung für diese Geräteklasse sein soll, hakt es bei den Clients immer noch bei vielen Details.
- Beim Laden von Webseiten zeigt sich, dass die Geschwindigkeit der Netzanbindung nicht die größte Rolle spielt.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

schlüsselte Verbindung ins Firmennetz aufbaut. Im Test kam er mit vielen CSS- und Javascript-lastigen Seiten gut zurecht. Im Detail stimmte nicht jede Position, aber damit muss man auch bei Desktop-Browsern rechnen.

Webseiten lassen sich lokal speichern, und zwar in den „Nachrichten“, also zwischen den E-Mails. Naheliegender wäre vielleicht der Zugang über das Menü des Browsers, etwa im Abschnitt „Lesezeichen“. Als einziger Testkandidat erlaubt der Bold das Einfügen von Kopiertem in das Wählprogramm. Dadurch lassen sich Telefonnummern von Webseiten aus relativ simpel anrufen – ohne den Umweg über Stift und Papier.

IMAP-Accounts kann der Bold verwenden, wobei die Passwort-Eingabe wie an fast allen Stellen unhandlich ist. Denn das Gerät zeigt wie Windows Mobile für jede gedrückte Taste sofort ein Sternchen an. Der Anwender erhält anders als beim E71 und beim iPhone keinen visuellen Hinweis auf das eingegebene Zeichen, nicht einmal für kurze Zeit. Das führt gerade bei virtuellen und kleinen Tastaturen zu Fehleingaben. Ob das Umwandeln in Sternchen bei einem so kleinen Bildschirm überhaupt nötig ist, erscheint ohnehin fraglich (und beim WLAN-Passwort fehlt es auch). Eine direkte Verbindung zu Exchange- und IMAP-Servern gibt es nicht, der Weg führt immer über den BES oder sein Äquivalent beim Mobilfunk-Provider. RIM begründet dies damit, dass so nur IP-Verkehr entsteht, wenn tatsächlich Daten zu übertragen sind – anders als beim ständigen Polling durch das Handy.



RIMs Blackberry Bold ist das erste Gerät des Herstellers, das UMTS und WLAN bietet (Abb. 1).

Der Ordner als unbekanntes Wesen

Von Mail-Ordnern auf dem Server will der Blackberry nichts wissen; er zeigt lediglich die Inbox. Folglich ist das Verschieben oder Kopieren von Mails in andere Folder nicht möglich, nur das lokale Speichern. Beim Beantworten von Nachrichten lässt sich das Original nicht kürzen, sondern höchstens insgesamt entsorgen. Per Mail-Client kann man im Betreff und im Absender suchen, weitere Möglichkeiten bietet das separate Suchprogramm.

Filter für Mail-Server offeriert nur der Exchange/BES-Client: Mit ihnen kann man festlegen, welche Nachrichten den Blackberry erreichen. Das Anzeigen von Anhängen übernehmen mitgelieferte Mini-Word-, -Excel-, und -Powerpoint-Anwendungen. Sie ermöglichen es (in engen Grenzen) Dokumente zu bearbeiten, allerdings keine neuen zu erstellen. Bei PDFs hingegen schwächelt RIM: Der BES konvertiert sie offenbar in Grafiken, sodass Texte wegen visueller Artefakte nur schlecht zu lesen sind.

Zertifikatsspeicher und VPN-Client

Termin- und Adressverwaltung sind ebenfalls vorhanden. Teilnehmer kann man nur mit einer gleichzeitig per Mail versandten Einladung zu Terminen hinzufügen. Für Kontaktdaten, Aufgaben und Verabredungen gibt es die Kategorien „persönlich“ und „geschäftlich“, weitere lassen sich definieren. Im Adressbuch kann man nur nach Vor-, Nach- und Firmennamen suchen. Für alles andere sollte eine externe Anwendung zuständig sein, die auch Mails und andere lokal gespeicherte Daten durchforstet. Im Test fand sie jedoch Städtenamen nur in den Nachrichten, nicht in Kontaktdaten oder Terminen.

Als Schmankerl legt RIM einen Passwort-Manager bei, der Zugangsdaten mit einem einzigen Kennwort verschlüsselt speichert. Verglichen mit handelsüblichen Programmen dieser Art handelt es sich um ein recht spartanisches Produkt, aber immerhin ist es da. Außerdem benutzt das Gerät einen internen Zertifikatsspeicher, in dem es unter anderem SSL-Zertifikate ablegt, der ebenso mit einem Passwort geschützt ist. Für sichere Verbindungen per WLAN in die Firma gibt es einen VPN-Client, der Gegenstellen verschiedener Firmen unterstützt (unter anderem Alcatel, Checkpoint, Cisco und Lucent).

Zur Bedienung stehen die Tastatur sowie ein Scrollball zur Verfügung, mit dem man auch Umlaute und andere akzentuierte Zeichen auswählt. Er ermöglicht schnelles Navigieren auf Webseiten und in Dialogen. Auf hierarchische Menüs verzichtet der Blackberry weitgehend, was die Navigation vereinfacht, aber einige recht lange Menüs produziert.

Die Oberfläche des Blackberry Bold ist zwar nicht verspielt, aber langsam schwindet der raue Charme aus TTY-Zeiten, den frühere Geräte ausstrahlten. Die Icons sind klar und gut zu erkennen. Die Aufteilung der Einrichtungsparameter auf drei davon („Einrichten“, „Optionen“ und „Verbindungen verwalten“) erscheint jedoch willkürlich und wenig hilfreich. Endlich verdient die installierte Schrift diese Bezeichnung, die Zeichen sind gut les- und unterscheidbar. Ähnlich wie beim E71 und dem Touch Diamond ließe sich die Bedienung der Anwendungen durch Icons für häufig benötigte Funktionen beschleunigen, allerdings fiele ihnen der knappe Bildschirmplatz zum Opfer. Das Scrollrad und einige speziellen Tasten erlauben zwar relativ schnelles Navigieren, die Suche in den wenig gegliederten und langen Menüs kostet jedoch wiederum Zeit. An einigen Stellen hat RIM deshalb Kurzmenüs eingeführt, die durch Klicken des Scrollrads erscheinen. Außerdem gibt es für viele Programmfunktionen einen direkten Zugang per Tastendruck. Die auf dem Gerät installierten Hilfetexte erklären diese Abkürzungen – vorbildlich.

Nokia E71

Mit seinem „Communicator“ führte Nokia vor Jahren das erste Smartphone überhaupt ein: Ein mit einem Handy integrierter Personal Digital Assistant. Einen Communicator gibt es immer noch, ins Rennen schickten die Finnen jedoch das handlichere E71 (s. Abb. 2). Es läuft mit Symbian 9.x, S60 3rd Edition. Allerdings bedeutet ein und

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Smartphones: Modelle und Ausstattung

Modell	Blackberry Bold	E71	Diamond Touch	iPhone 3G
Hersteller	Research in Motion	Nokia	HTC	Apple
Betriebssystem	Blackberry OS 4.6	Symbian 9, S60 3rd	Windows Mobile 6.1	iPhone OS 2.0
Maße (mm^3)	114 × 66 × 16	114 × 57 × 10	102 × 51 × 11	116 × 62 × 12
Gewicht (g)	136	127	110	133
RAM	1 GByte	110 MByte	192 MByte/4 GByte	16 GByte
Display (Größe/Pixel/Farben)	2,2"/480 × 320/65000	2,36"/320 × 240/16,7 Mio	2,8"/640 × 480/16,7 Mio	3,5"/480 × 320/k. A.
Tastatur	✓	✓	–	–
Laufzeit h (Standby/Gespräch/3G)	312/5/k. A.	480/10/4	396/5,5/4,5	300/10/5
externer Speicher (Format/Max.)	microSD/32 GByte	microSD/8 GByte	–	–
Bluetooth/IR	✓/–	✓/✓	✓/✓	✓[6]/–
Mail-Protokolle	IMAP, POP3, SMTP[2], RIM-eigenes	POP3, IMAP, SMTP, Activesync Exchange	POP3, IMAP, SMTP, Activesync Exchange	POP3, IMAP, SMTP, Activesync Exchange
Exchange-Folder	–	–	✓	✓[7]
Exchange-Offline[1]	LAW	LAW	LAWV	AW
IMAP-Folder	–	✓[5]	✓	✓[7]
IMAP-Offline[1]	LAW	LAW	LAWV	LAWV
Office-Anhänge	betrachten/bearbeiten	betrachten/bearbeiten	betrachten/bearbeiten	betrachten
Backup-Programm	–	✓	✓	–
PPTP	–	–	✓	✓
L2TP	–	–	✓	✓
IPSec	✓[3, 4]	✓[3]	✓[3]	✓[3]
Website	www.blackberry.de	www.nokia.de	www.htc.com	www.apple.de

[1]L: Löschen, A: Antworten, W: Weiterleiten, V: Verschieben; [2]via HTTP-Proxy; [3]nur mit bestimmten Gateways; [4]außerdem implizit bei Nutzung des Blackberry Enterprise Servers; [5]kein Verschieben und Kopieren zwischen IMAP-Foldern; [6]alle vorhandenen Folder, keine Abonnements möglich; [7]nur für Headsets nutzbar

dasselbe Betriebssystem bei Handys noch lange kein identisches Aussehen oder identische Bedienung. So unterscheidet sich das E71 in vielen Details vom im letzten Jahr erschienenen E61i, das mit dem gleichen Betriebssystem läuft.

Gegenüber seinem Vorgänger reagiert es deutlich schneller, man hat nicht mehr das Gefühl, dass es jeden Programmstart erst gründlich überlegen müsse. Die Tastatur lässt sich dank eines deutlichen Druckpunkts angenehmer und sicherer bedienen, obwohl sie einen Zentimeter schmaler und die Tasten entsprechend kleiner sind. Es gibt nur noch eine Umschalttaste, die ebenso wie die für das Aktivieren der zweiten Belegung (Ziffern und einige Sonderzeichen) links neben der Leertaste angeordnet ist.



Das E71 von Nokia benutzt zwar dasselbe Betriebssystem wie das ältere E61, reagiert jedoch wesentlich schneller (Abb. 2).

Man kann nicht oft genug fragen

IMAP-Server lassen sich als E-Mail-Quellen definieren, dabei muss man alle Verbindungsparameter von Hand eingeben; ebenso wie beim Anschluss des SMTP-Servers erkennt das Gerät nicht selbsttätig, dass er SSL/TLS verwendet. Diese Einstellungen sind immerhin nur einmal nötig; anders als die Wahl der Internetverbindung. Statt automatisch mit einem bekannten WLAN-Zugangspunkt zu verbinden (was meist schneller und billiger als ein GPRS/UMTS-Zugang sein dürfte), fragt das Gerät jedes Mal nach, ob sein Eigentümer denn nun per Mobilfunk oder drahtlosem LAN ins Netz wolle. Ist keine SIM-Karte installiert, stellt es sogar die putzige Frage „WLAN-Verbindung im Offline-Modus erstellen“. Wer wirklich ins Netz will, muss hier „Ja“ wählen, als ob eine WLAN-Verbindung offline funktionieren könnte.

Auch bei der Anbindung des Exchange-Servers zeigt sich das E71 wenig flexibel: Im „Profil“ muss man den Zugangspunkt fest einstellen. Das stört bei wechselnden WLAN-Accesspoints, denn vor dem Synchronisieren der Daten ist jedes Mal eine Änderung des Profils nötig. Ebenso ärgerlich fällt die Behandlung von SSL-Zertifikaten aus: Verwendet der Server ein selbstsigniertes, darf der Benutzer wie üblich wählen, ob er es einmalig, für immer oder gar nicht akzeptieren will. Dumm nur, dass „für immer“ keine sinnvollen Folgen hat. Einmalig akzeptierte Zertifikate scheinen mit einem Ablaufdatum versehen zu sein, so fragt der Browser teilweise mitten beim Laden einer Seite wiederum nach, ob man ihm vertrauen wolle. Das alles ist überflüssig und nervt ebenso wie die obskure Meldung „WLAN bereits aktiv, bitte schließen und erneut versuchen“. Sie erscheint beim Versuch, während einer laufenden Exchange-Synchronisation Mail vom IMAP-Server herunterzuladen. Ins Web darf man aber trotzdem.

Wie erwähnt, hängen die anderen WLAN-fähigen Geräte das E71 beim Darstellen von Webseiten locker ab. Es bietet jedoch die Möglichkeit, einmal Geladenes lokal zu speichern. Das könnte Tempo-Vorteile bringen. Wenn die Funktion denn brauchbar implementiert wäre: Im Test dauerte das Laden der Spiegel-Seite aus dem lokalen

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Speicher mit 40 Sekunden doppelt so lange wie via WLAN.

Raum für Verbesserungen gibt es zudem beim Exchange-Client. Bei sehr vielen ungelesenen E-Mails (im Test über 600) bremst er sämtliche Mail-Funktionen aus. Das Konzept von Ordnern ist spurlos an ihm vorbeigerauscht: Mails kann man nur in lokale Verzeichnisse auf dem Telefon verschieben, Unterordner auf dem Exchange-Server erscheinen auf dem E71 nicht. IMAP-Folder lassen sich zwar abonnieren und relativ normal bearbeiten; ein Kopieren oder Verschieben von Mails zwischen ihnen ist allerdings unmöglich. Nokia hat sogar Software zum Bearbeiten von Word- und Excel-Dokumenten installiert.

Immerhin lassen sich Mails mit einer separaten Anwendung durchsuchen. Allerdings fahndet sie unbeirrbar in der gesamten Nachricht und allen anderen Dateien auf dem Gerät nach der eingegebenen Zeichenkette. Eine parametrisierbare Suche im Mail-Client wäre hilfreicher. Zumal die erwähnte Anwendung ähnlich wie ein Web-2.0-Programm nach den ersten paar Buchstaben mit der Suche beginnt – das bremst den Anwender unnötig aus, der mit seiner Eingabe womöglich noch gar nicht fertig war.

Die üblichen PIM-Funktionen bringt Nokias Smartphone mit, sie schwächeln jedoch im Detail. So gibt es keine brauchbaren Kategorien für Kontaktdaten, und solche Zuordnungen etwa in Outlook oder Exchange verschwinden beim Synchronisieren. Zwischen Terminen und Teilnehmern an ihnen gibt es keine Verbindung, das Suchen in Terminen erlaubt nur die erwähnte externe Anwendung. Groteske Folgen zeitigt ein seit Jahren in Symbian S60 gehätschelter Bug: Wer seine Uhrzeit umstellt, weil er sich in einer anderen Zeitzone befindet, dem „korrigiert“ die Software automatisch alle Termine.

Ist etwa der Abflug wie üblich in der jeweiligen Ortszeit eingetragen, riskiert man dadurch, etliche Stunden zu spät am Flughafen zu erscheinen. Einziger Ausweg: Nie die Zeit auf dem Smartphone umstellen und „Zeit vom Netzbetreiber beziehen“ abschalten, um automatische Änderungen zu verhindern. Pfiffig beschleunigt ist hingegen das Wählen von Telefonnummern: Durch Drücken einer Taste auf der alphanumerischen Tastatur erscheint außer der ihr zugeordneten Ziffer eine Liste aller Kontakte, die mit dem jeweiligen Buchstaben beginnen. Daraus kann man schnell den gewünschten auswählen und anrufen.

VPN-Konfiguration mit viel Aufwand

Eine mitgelieferte Backup-Anwendung ermöglicht die Datensicherung auf einer Micro-SD-Karte, die sich an der Seite des Telefons einschieben lässt. Im Test speicherte das Programm nicht nur die Nutzerdaten, sondern auch separat installierte Anwendungen. Im Prinzip sollte man also ohne Nokias PC-Suite jederzeit eine komplette Datensicherung anlegen können.

Einen IPSec-Client bringt das E71 zwar mit. Konfigurieren lässt er sich jedoch nur, wenn der Betreiber des VPN-Gateway geeignete Dateien per HTTP bereitstellt. Deren Format ist zumindest bei Nokia nicht dokumentiert. Nach Berichten im Web lassen sich die nötigen Parameterdateien alternativ manuell auf einem PC erstellen. Allerdings kann man sie erst nach dem Signieren mit einem Symbian-Entwicklerzertifikat auf dem Smartphone installieren. Dieser Prozess ist umständlich und langwierig, außerdem lässt er sich nur auf einem Windows-PC erledigen. Für eine simple VPN-Konfiguration deutlich zu viel Aufwand.

Zur Bedienung des E71 steht neben der Tastatur eine zentral unter dem Bildschirm platzierte Vier-Wege-Wippe zur Verfügung. Mit ihr wählt man zu startende Programme aus und bewegt den Mauscursor in Webseiten. Das funktioniert zuverlässig, allerdings langsamer als das direkte Anklicken bei einem Touchscreen. Die Benutzerführung erfolgt ausschließlich durch Menüs, deren erste Option häufig auf den Knopf der Wippe gelegt ist. Das beschleunigt das Arbeiten zwar etwas, grafische Elemente zum Antippen würden jedoch den Zugang zu oft benötigten Funktionen erleichtern. Beim Tippen hilft eine zuschaltbare Vervollständigungsfunktion. Sie übernimmt neue Wörter auf Wunsch in ihre Liste.

iX-Wertung

Blackberry Bold

⊕ Onlinehilfe auf dem Gerät
⊕ Mail-Filter für Exchange-Account
⊕ Copy & Paste aus Webseiten

⊖ Schwächen beim Suchen
⊖ keine Exchange/IMAP-Folder

Nokia E71

⊕ Suche in Dokumenten, Kontaktdaten und Terminen
⊕ Bearbeitung von Office-Dokumenten
⊕ Textvervollständigung

⊖ langsamer Browser
⊖ uralter Fehler bei der Zeitumstellung
⊖ kein PPTP/L2TP

HTC Touch Diamond

⊕ klein und leicht
⊕ Exchange/IMAP-Folder
⊕ teilweise komfortable Bedienung

⊖ verspielte GUI-Ideen
⊖ fummelige WLAN- und Internet-konfiguration

iPhone 3G

⊕ komfortable Bedienung
⊕ großes Display
⊕ schneller Browser

⊖ Schwächen im Offlinebetrieb
⊖ lückenhafte PIM-Funktionen
⊖ keine Ordner-Abonnements

HTC Touch Diamond

Als Erstes fallen beim Touch Diamond des taiwanischen Herstellers HTC Form und Farbe auf: Von der Verpackung bis zum Handy zieht sich das Motiv des schwarzen Pyramidenstumpfs (Abb. 3). Unter dem Bildschirm sitzt ein vom iPod inspiriertes Rad zur Steuerung.

Auf dem Gerät läuft Windows Mobile 6.1, wovon man allerdings zunächst nichts merkt. Denn die von HTC entwickelte Oberfläche „Touch Flo 3D“ bewahrt den Anwender erst einmal vor dem eher spartanischen Unterbau. Navigiert wird wie auf dem iPhone mit den Fingern durch Überstreichen des Bildschirms und Antippen des gewünschten Programms. Das ist ein wenig gewöhnungsbedürftig, da große Finger auf dem kleinen Bild-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

schirm die Icons nicht immer zuverlässig treffen. Im Zweifelsfall hilft der an der Seite des Geräts versenkte Stift, das Gewünschte zuverlässig auszuwählen. Ebenfalls wie beim iPhone registriert das Telefon, ob sein Benutzer es hoch oder quer hält und dreht gegebenenfalls den Bildschirminhalt.

Sinnvoll und leicht zu bedienen sind die von HTC geschaffenen Elemente zum An- und Abschalten von Funk-Interfaces: Es reicht, einen virtuellen Schieber nach rechts oder links zu bewegen, um das jeweilige Netz einoder auszuschalten. Bei der Mail-Anzeige verschlechtert das Modische aber den Gebrauchswert. Ein aufgeklappter Briefumschlag, in dem der Anfang der Nachricht zu erkennen ist – das sieht zwar putzig aus, die Mikro-Schrift dürfte aber nur noch für Raubvögel im Tiefflug lesbar sein. Vollends sinnfrei stellt sich Touch Flo bei der Kontaktverwaltung dar: Die elegante Auswahl per Fingerzeig funktioniert nur mit den Personen, für die ein Foto hinterlegt ist. Das ist im Geschäftsbetrieb vermutlich die Ausnahme. Folglich bleibt für das Finden von Kontaktdaten nur der übliche Weg über die Windows-Mobile-Oberfläche: Eintippen des gesuchten Namens oder Blättern. Alternativ steht eine externe Anwendung zum Suchen zur Verfügung, die beliebigen Text in allen Feldern der Kontakt- oder Termindaten findet.

Tippt man das Blatt im aufgeklappten Mail-Umschlag an, erscheint die in Windows Mobile übliche Listenansicht der eingegangenen Mails. Hier erfolgt die Bedienung wie gewohnt: Menüeinträge rechts unten aktivieren, rechts oben „OK“ klicken oder das Fenster schließen, Optionen für einzelne Mails durch länger dauerndes Antippen aktivieren. All das ist grundsolide aber gelegentlich etwas mühsam – wie schon immer bei Windows Mobile.

Erwartungsgemäß funktioniert die Anbindung an einen Exchange-Server ohne Mucken und Murren, sogar einzelne Unterordner lassen sich für das Synchronisieren auswählen. Dem Mail-Client ist es gleichgültig, ob gerade eine Netzverbindung besteht. Gegebenenfalls merkt er sich alle Änderungen und führt sie aus, wenn der Exchange-Server wieder erreichbar ist. Mail-Anhänge in den üblichen Büroformaten stellen keine Hürde für das Touch Diamond dar. Mit den installierten Mini-Versionen von Word und Excel lassen sich einige einfache Arbeiten an Dokumenten erledigen. Beim IMAP-Client



Kleinstes Gerät im Test war das Touch Diamond von HTC, auf dem Windows Mobile 6.1 läuft (Abb. 3).

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

hat Windows Mobile die Nase vorn: Als einziger im Test erlaubt er das Abonnieren von Ordnern. Nachrichten kann man zwischen ihnen verschieben, und ebenso wie beim Exchange-Client lassen sich alle Arbeiten trotz fehlender Netzverbindung ausführen.

Weniger überzeugend fällt nach wie vor die Internetanbindung aus. Das Verbinden mit einem WLAN-Accesspoint funktionierte zwar irgendwann. Es war aber kaum auszumachen, warum viele nach eigenem Empfinden identische Versuche vorher scheiterten. Brauchbare Fehlermeldungen gibt es nicht, und die Onlinehilfe hilft nicht. Wie in den ersten Tagen von Windows Mobile muss man sich mit der Frage beschäftigen, ob eine WLAN-Verbindung „ins Internet“ oder „in die Firma“ führt. Wer das wozu wissen will, bleibt unklar. Schließlich gibt es doch einen PPTP- und einen L2TP/IPSec-Client auf dem Gerät, mit dem man sicher „in die Firma“ gehen kann, während man gerade „im Internet“ ist. In dieser Hinsicht sind Apple, Nokia und RIM deutlich weiter.

Das Gerät hatte von allen im Test die kleinsten Abmessungen. Wie bei anderen Handys mit Windows Mobile ersetzt eine virtuelle Tastatur die fehlende physische. Das Betriebssystem blendet sie ein, sobald man mit dem Stift ein Eingabefeld aktiviert. Das HTC bietet außer der üblichen weitere Tastaturvarianten an, unter anderem eine mit größeren, allerdings mehrfach belegten Tasten. Sie verhält sich ähnlich wie ein klassisches Handy mit eingeschaltetem T9.



Apples iPhone 3G funkt mit halber HSDPA-Geschwindigkeit und synchronisiert seine Daten mit Exchange-Servern (Abb. 4).



iPhone 3G

Zu der grafischen Oberfläche des iPhone (s. Abb. 4) gibt es kaum Neues zu sagen – das Meiste existierte so schon in der Vorgängerversion [1], die noch kein UMTS beherrschte. Auffälligste Ergänzung ist das mit der Version 2 des Betriebssystems eingeführte Löschen und Verschieben mehrerer E-Mails auf einmal. Dazu klickt man in der Mail-Übersicht auf „Bearbeiten“, worauf vor jeder Nachricht eine Checkbox erscheint.

Copy und Paste sind immer noch nicht möglich, deshalb kein komfortables Wählen aus einer Webseite oder einem Dokument heraus, kein Übertragen von Daten zwischen Anwendungen. Die bereits an der Vorgängerversion kritisierte lückenhafte Länderliste ist ebenso unvollständig wie vorher – wohl dem, der keine Menschen in Litauen, Estland oder Malaysia kennt. Im Test stürzte das Gerät mehrmals nach schnellem Scrollen auf einer Webseite ab. Die Arbeit mit IMAP-Servern funktioniert, allerdings zeigt das iPhone immer alle auf dem Server existierenden Ordner. Daran lässt sich nichts ändern, denn IMAP-Abonnements kennt es nicht.

Für Business-Kunden relevant ist die neue Exchange-Anbindung. Sie funktionierte im Test reibungslos, im Detail gibt es aber Verbesserungsmöglichkeiten. So ist es nicht möglich, Exchange-Mails zu löschen oder zu verschieben, wenn gerade keine Internetverbindung besteht. Damit hatte die Konkurrenz im Test keine Schwierigkeiten. Mit IMAP-Mails funktionieren alle Operationen auch offline. Allerdings führt das iPhone etwa das Verschieben in einen anderen Ordner erst aus, wenn der Anwender das nächste Mal das IMAP-Postfach öffnet. Wer sich dafür entscheidet, Termine und Kontaktdaten mit Exchange zu synchronisieren, verliert beim ersten Mal alle lokalen Daten dieser Art.

Ebenfalls an Geschäftskunden richtet sich der IPSec-Client, den Apple jetzt mitliefert. Er verwendet den „aggressive mode“ zur Schlüsselaushandlung, und das lässt sich nicht umstellen. Da keine geeignete Gegenstelle zur Verfügung stand, war kein Test dieser VPN-Variante möglich. Weiterhin verfügbar sind PPTP- und L2TP-Clients.

Größte Neuerung für alle Anwender ist das sich im Namen widerspiegelnde UMTS, mit dem das iPhone beim Herunterladen bis zu 3,6 Mbps erreichen soll. Beim Anzeigen von Webseiten zeigt es sich damit etwa gleich flott wie das nominell doppelt so schnelle Touch Diamond. Das scheint, wie auch beim Webseitenabruf via WLAN, vor allem an Apples Webkit-Browser zu liegen.

Bei den PIM-Anwendungen hat sich nichts getan, was für professionelle Nutzer wichtig wäre. Eine Aufgabenverwaltung liefert Apple nach wie vor nicht. Der iTunes-Store hält, wen wundert's, besonders viele Programme dafür bereit. Installieren lassen sie sich drahtlos durch Knopfdruck. Beim nächsten Anschließen des Telefons an den Desktop lädt iTunes diese Anwendungen auf die lokale Festplatte.

Fazit

Zwar heißt es immer wieder, Smartphones seien nun wirklich reif für den professionellen Einsatz. Ein Blick auf die verfügbaren Geräte zeigt jedoch, dass es an der einen oder anderen Stelle immer noch hakt. Mal ist der Browser langsam, mal gehen beim Abgleich mit dem Server oder Desktop Daten verloren, mal ist die Bedienung mühselig, mal die Anzeige von Webseiten fehlerhaft. Häufig fehlen banale Funktionen, die das Leben unterwegs erleichtern würden, etwa das Übernehmen einer Telefonnummer oder Anschrift aus einer Webseite in eine andere Anwendung. Selbst bei dem laut Geräte- und Betriebssystemherstellern wichtigsten Einsatzgebiet E-Mail fehlt noch einiges, von Signatur und Verschlüsselung via S/MIME oder PGP/GnuPG wagt man gar nicht zu träumen. Wer jetzt das passende Smartphone für die Firma sucht, muss vor allem entscheiden, worauf er verzichten kann. (ck)

Literatur

[1] Christian Kirsch; Mobile Computing; Kleine Erleuchtung; Apples iPhone als Geschäftstelefon; *iX* 1/08; S. 68

[2] Christian Kirsch; Smartphones; Halb und Halb; Blackberry Curve und Nokia E90 im Test; *iX* 9/07, S. 78





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Im Vergleich: Crystal Reports Server 2008 und BIRT

Datenpressen

Joachim Nelz, Juri Urbainczyk

Open-Source-Software erobert zunehmend Felder, in denen es zu kommerziellen Produkten lange kaum Alternativen gab. Im Unternehmensreporting konkurriert beispielsweise das Eclipse-Projekt BIRT ernsthaft mit traditionellen Werkzeugen wie Crystal Reports.

Wie bei vielen IT-Entscheidungen stellt sich auch vor der Anschaffung eines Reporting-Werkzeugs die Frage: Kaufen oder sich in der Open-Source-Szene umsehen? Eine eindeutige Antwort gibt es in der Regel nicht, vielmehr hängt die Entscheidung stark vom Einsatzzweck ab. BIRT (Business Intelligence and Reporting Tools) und Crystal Reports Server 2008 sollen hier als typische freie beziehungsweise kostenpflichtige Vertreter unter die Lupe genommen werden – und zwar im Kontext großer Entwicklungsprojekte (alle Onlinequellen sind über den *iX*-Link am Ende des Textes zu erreichen).

Das weit verbreitete Crystal hat schon viele Jahre und einige Besitzerwechsel hinter sich. Zurzeit entwickelt es der französische BI-Spezialist Business Objects weiter, der seinerseits Anfang dieses Jahres von SAP aufgekauft wurde, als eigenständiger Geschäftsbereich aber weiter besteht. Zwar gibt es inzwischen mit Crystal Reports for Eclipse eine Java-Variante, das Werkzeug verleugnet seine Windows-Affinität jedoch nicht. Seit 2004 führt die Eclipse-Community das in Java geschriebene BIRT als Top-Level-Projekt.

Beide Werkzeuge bieten eine Entwicklungsumgebung mit Preview-Funktion sowie eine Webanwendung (Viewer) zum Ausführen der Reports. Beide speichern die Reports inklusive aller relevanten Informationen, etwa Datenbankverbindungen und Formatierungen, in Dateien. Während Crystal mit Binärdateien arbeitet, die auch Nutzdaten enthalten können, legt BIRT seine Reports in XML-Dateien ab, die besser vergleichbar und einfacher zu versionieren sind. In beiden Umgebungen erstellt der Entwickler die Reports auf seinem lokalen PC. Ein Konfigurationsmanagementsystem verfrachtet die Ergebnisse anschließend auf den Server (Abbildung 1).

Crystal: Ohne SQL bedienbar

Wer mit Crystal einen Report erstellen will, muss zunächst eine Datenbankverbindung etablieren. Das Werkzeug bietet davon eine große Auswahl, der Standardmechanismus ist ODBC. Für einen Report kann der Entwickler mehrere Verbindungen festlegen. Er wählt die gewünschten Tabellen aus und stellt bei Bedarf Relationen zwischen ihnen her. Um den Report mit Daten zu füllen, genügt es, Datenbankfelder per Drag & Drop hineinzuziehen. SQL-Kenntnisse braucht man nicht, Crystal generiert das entsprechende Statement automatisch, an dieser Stelle ist ein manueller Eingriff nicht möglich. Ebenso schnell lassen sich hierarchische Gruppen (Aggregationen) erzeugen (Abbildung 2). Die Vorschau zeigt den ausgefüllten Report.

Ein Report besteht aus mehreren vertikal untereinander liegenden Bereichen (Berichtskopf, Seitenkopf et cetera). Jede neue Gruppe fügt Gruppenkopf und Gruppenfuß ein. Alle Elemente befinden sich in einem dieser Bereiche, beispielsweise der Titel im Berichtskopf. Dadurch bestimmt sich die Lage und teilweise die Formatierung dieser Elemente.

Formatierungen für Datentypen wie Datum und Zeit stellt der Entwickler über ein Menü ein. Dass die Konfigu-

iX-TRACT

- Das freie BIRT sowie das kostenpflichtige Crystal Reports sind prominente Vertreter zweier unterschiedlicher Herangehensweisen an das Unternehmensreporting.
- BIRT ist ein ambitioniertes und leistungsfähiges Eclipse-Projekt, das sich für große Vorhaben eignet, allerdings großen Lerneinsatz erfordert.
- Mit Crystal Reports kann auch ein Anwender etwas anfangen. Es hilft beim Erstellen von Ad-hoc-Reports und generiert SQL-Abfragen automatisch.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

PRD_9999_Dimension_CRS_Organisationsstruktur

Druckdatum: 10.04.2008
Daten geladen am:07.04.2008

Parameter: Kostenstelle_Fachkey = *

Regionalstruktur	Kostenstelle	Firma	Divisioı
RVSO Aussenorganisation			
RSC Region Stapler			
RSC1 Region Stapler			
R301 Stap. Hamburg			
R301A AD Stap Hamb			
	30120 Admin Stap Hamburg	10	ZBM
R301S Se. Stap Hamb			
	30162 ID / Werkstatt Stap Hamburg	10	ZBM
	30161 Ersatzteil Stap Hamburg	10	ZBM
	30163 Aussend Stap Hamburg	10	ZBM
	30160 Service Stap Hamburg	10	ZBM
R301V VK Stap Hamb			
	30145 GM Verkauf Stap Hamburg	10	ZBM
	30140 Verkauf Stap Hamburg	10	ZBM
	30146 GM Verkauf Stap Hamburg	10	ZBM
	30144 NM Verkauf Stap Hamburg	10	ZBM

Mit Crystal lassen sich schnell Reports mit mehreren Aggregationen anlegen (Abb. 2).

ration auch zur Serverumgebung passt, muss er allerdings manuell sicherstellen. Zum Formatieren der Elemente gibt es einen speziellen Editor, in dem man beispielsweise Farben, Rahmen, Fonts und Ausrichtung anpasst sowie via Hyperlink eigene Navigationselemente in den Report integriert. Es zeugt von Crystals oft wenig durchdachten Grundkonzepten, dass Letzteres im Format-Editor geschieht.

Nach der Selektion der Elemente bietet der Editor nur noch die Formatierungen an, die für alle ausgewählten gleichermaßen verfügbar sind. So lassen sich im Prinzip viele Elemente gleichzeitig ändern – jedoch funktioniert das nur dann, wenn die Ausgangswerte gleich sind. Crystal erlaubt das Ausrichten der Elemente an anderen oder an Tabulatorpositionen. Leider gibt es keine Möglichkeit, sie hierarchisch zu strukturieren, was das Positionieren von Gruppen aufwendig macht. Schmerzlich vermisst man Boxen, die weitere Elemente aufnehmen können und Formatierungen vererben. Viele der Formatierungs- und Steuerungsoptionen legt der Anwender entweder beim Entwickeln fest oder bestimmt sie zur Laufzeit dynamisch per Skript. Beispielsweise ließe sich die Hintergrundfarbe eines Bereichs zur Laufzeit anpassen (in Crystal- oder Visual-Basic-Syntax):

```
if Remainder(RecordNumber,2) = 0 then
crWhite else crHellgrau
```

Die Formel teilt die Farbe abhängig von der aktuellen Satznummer zu. Ebenso ließen sich Felder (Limits) hervorheben, Bilder abhängig von Bedingungen anzeigen oder Gruppierungs- und Selektionskriterien definieren und anderes mehr.

BIRT: Ohne SQL geht nichts

Auch unter BIRT muss der Entwickler zuerst eine Datenbankverbindung etablieren, im Normalfall via JDBC. Wenn der Report im Viewer läuft, lässt sich hierfür das Connection-Pooling des JEE-Containers nutzen, was die Migration in unterschiedliche Umgebungen erleichtert. Neben relationalen Datenbanken kann BIRT auch andere Quellen anzapfen, etwa Flat Files, XML-Dateien und Scripted Datasources. Letztere behandeln Java-Klassen als Datenquelle und stellen einen generischen Integrationsansatz dar. Als Basis eines typischen Reports dient eine SQL-Anfrage (Data Set), die man um zusätzliche berechnete Spalten erweitern kann. Die Anfrage muss der Anwender, anders als bei Crystal, manuell stellen. Aus den Data Sets entwickelt er die Anzeigeelemente: Das Ziehen eines Data Set auf den Report erzeugt beispielsweise eine Tabelle.

Die sogenannte Master Page, in der Seitenformat, Seitenränder sowie Kopf- und Fußzeile eingetragen sind, bestimmt zunächst das Layout. Weiterhin besitzt jeder Report ein „Theme", das eine Sammlung von Styles enthält (Schriftart, Hintergrund, Rahmen et cetera). Hier lassen sich Formatierungsregeln für Strings, Zahlen und Datum festlegen. Der Entwickler arbeitet entweder mit den vorgefertigten Styles (etwa für Tabellen) oder erstellt eigene.

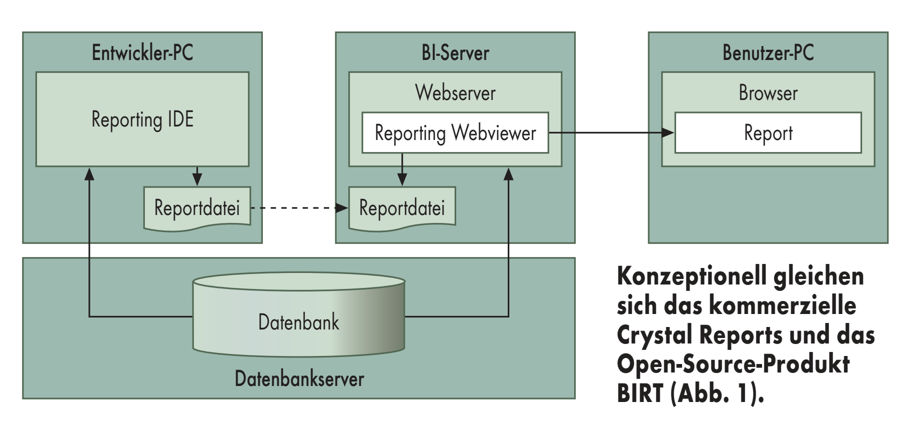
Bilder kann man auf verschiedene Arten einbinden, nämlich als URI, Shared Resource File (gemeinsame Datei), Embedded Image (im Report integrierte Image-Daten) sowie Dynamic Image (Image aus einer SQL Query). Hier lauern noch einige Fallstricke, da sich je nach Ausgabeformat abhängig von der Auflösung die Bildgröße ändert. Als unproblematisch haben sich Embedded Images erwiesen. Ausgaben in HTML und PDF funktionieren einwandfrei; aufwendige Layouts erzeugen in Office-Formaten wie Excel oder Word ebenso wie Postscript oftmals Schwierigkeiten.

Jedes Element (Tabelle, Textfeld et cetera) besitzt eigene Layouteigenschaften, die ähnliche Möglichkeiten wie Styles bieten. Diese Formatierungen sind jedoch im Gegensatz zu Styles nicht wiederverwendbar, weswegen man Letzteren den Vorzug geben sollte. Es ist möglich, die Elemente flexibel zu positionieren, hierzu dient eine Layouttabelle (Grid), die in der Lage ist, beliebige Elemente aufzunehmen.

Generieren oder programmieren

Zur dynamischen Steuerung des Reports bietet BIRT verschiedene Optionen. Die bedingte Formatierung erlaubt es, das Erscheinungsbild von Elementen anhand des Ausgabeformats oder beliebiger Ausdrücke festzulegen. Weiterhin lässt sich einem Element dynamisch ein Style zuweisen, etwa um negative Werte in roter Schrift darzustellen.

Bei der Anzeige eines Reports löst BIRT verschiedene Ereignisse aus, an



Konzeptionell gleichen sich das kommerzielle Crystal Reports und das Open-Source-Produkt BIRT (Abb. 1).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

iX-Wertung

Crystal Reports

⊕ kurze Einarbeitungszeiten
⊕ Ad-hoc-Reporting
⊕ Funktionsumfang
⊕ grafische Visualisierung

⊖ eingeschränkt modularisierbar
⊖ nur bedingt geeignet für große Projekte

BIRT

⊕ gute Modularisierbarkeit
⊕ unterstützt verteiltes Arbeiten
⊕ komplexe Auswertungen
⊕ Erweiterbarkeit

⊖ wenige Output-Formate
⊖ Layoutschwächen

Daten und Preise

Crystal Reports Server 2008

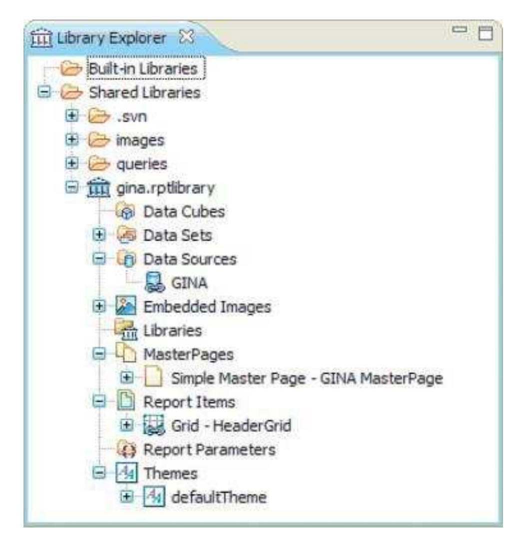
Preis: 1995 Euro für fünf Namenslizenzen, 4995 Euro für fünf Zugriffslizenzen

Anbieter: SAP (Business Objects), www.businessobjects.com/product/catalog/crystalreports_server/

BIRT 2.3

Lizenz: Eclipse Public License

BIRT-Projekt: www.eclipse.org/birt/phoenix/



BIRTs Report Libraries helfen vor allem in großen Projekten beim Modularisieren der Reports (Abb. 3).

die der Entwickler eigene, in Javascript geschriebene Event-Handler anhängen kann. Das folgende Beispiel zeigt den *beforeFactory()*-Event-Handler des Wurzelelements, der Variablen definiert. Alle folgenden Javascript-Ausdrücke können diese Variablen verwenden.

```
currentYear = currentDate.getFullYear();
beginDate = new Date(currentYear, 0, 1);
endDate = new Date(currentYear, 11, 31);
```

Trotz aller Unterschiede besitzen Crystal und BIRT einige Gemeinsamkeiten, etwa bei Parametrierung und Grafikeinbindung. Beide Werkzeuge können Parameter wie *Kunde* oder *Datum* verwenden, um Daten zu filtern oder die Struktur des Reports zu ändern. Die Werte stammen entweder vom Benutzer (Dialog) oder von der aufrufenden Anwendung (URL). Sowohl statische als auch dynamische Parameter sind erlaubt. Die Auswahl der Parameter aus einer Hierarchie (etwa „Land, Region, Stadt“ (Cascading Parameters) ist ebenfalls möglich. Um einen dynamischen Parameter zu erzeugen, gibt der Entwickler bei Crystal ein Datenbankfeld an, aus dem die Werte gelesen werden. Bei BIRT definiert er ein Data Set, das zur Laufzeit die Parameterwerte erzeugt. Während der BIRT-Anwender den Typ des Parameters konzeptionell bedingt manuell definiert, ergibt er sich bei Crystal automatisch aus dem Typ des Datenbankfeldes. Das führt gelegentlich zu Inkompatibilitäten, beispielsweise wenn der Report eine Jahreszahl – in der Datenbank vom Typ INT –, als Zahl interpretiert und daher mit einem Tausenderpunkt darstellt.

In Crystal verknüpft der Benutzer die Parameter mit der Datenabfrage via Dialog, indem er Selektionskriterien definiert, die das Werkzeug automatisch als SQL-Statement übernimmt. Vorsicht ist beim Löschen von Parametern geboten: Wenn man nicht alle Referenzen auf den Parameter entfernt hat, wird er nicht korrekt gelöscht – mit unvorhersehbaren Folgen. Bei BIRT spezifiziert der Entwickler im Data Set ein oder mehrere Platzhalter, die er dann an einen Report-Parameter bindet. So werden die Werte in die Query eingesetzt.

Beide Werkzeuge bieten eine große Auswahl an Grafiken wie Torten, Säulen und Linien. Crystal bringt 16 konfigurierbare Typen mit. Hier durchzusteigen ist nicht einfach, allein schon deshalb, weil nach Einfügen der Grafik fünf und mehr Dialoge mit mehreren Tabs zur Verfügung stehen. BIRT bietet dreizehn sogenannte Charts in jeweils ein bis drei Varianten an. Bei Auswahl und Konfiguration hilft ein übersichtlicher Wizard. Mit interaktiven Grafiken können beide Produkte aufwarten. BIRT erlaubt sogar, in unterschiedlichen Teilen der Grafik (etwa in einer Legende) verschiedene Aktionen durchzuführen.

In größeren Projekten stellt sich die Frage, wie sich bei einer großen Anzahl von Reports deren Konsistenz und Wartbarkeit gewährleisten lässt. Der Schlüssel liegt in der Modularisierung von Logik und Layout. Crystal-Reports kann der Entwickler in anderen Reports als Subreports verwenden. Dazu zieht er die gewünschte Auswertung auf eine geeignete Stelle im Hauptreport. Der Austausch von Daten ist in beide Richtungen möglich. Leider wird so stets eine Kopie des Subreports erzeugt. Änderungen am Original führen nicht zum automatischen Update des integrierten Subreports. Alternativ erstellt der Anwender einen „echten“ Link zu einem anderen Report: Da die URL hier dynamisch aufgebaut wird, ist es möglich, zur Laufzeit Parameter zu übergeben. Obwohl das Verlinken gut funktioniert, ist ein Aufteilen der Berichte in handliche Module so nur begrenzt realisierbar.

Kleine Häppchen für große Projekte

Crystal enthält ein Repository, in dem man beispielsweise Formeln zentral hinterlegt. Eine Alternative dazu bieten die in einer beliebigen .Net-Sprache implementierbaren User Function Libraries. Die Funktionsbibliotheken stellen Algorithmen und Daten bereit, auch ein Zugriff auf Konfigurationsdateien ist möglich. Zum Verwalten des Layouts stehen Templates bereit, auf deren Basis der Entwickler neue Reports aufbaut. Diese Vorlagen kann er zwar auch auf einen existierenden Report anwenden, die Ergebnisse sind aber – da abhängig von den verwendeten Funktionen und Formatierungen – nicht vorhersehbar. Grafiken und Bilder, die in vielen Reports zum Einsatz kommen (etwa Ampeln oder Logos) lassen sich via URL einbinden.

BIRT bringt zum Zwecke der Modularisierung das mächtige Konzept der Report Libraries mit. Sämtliche Elemente eines Reports können in einer

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

solchen Bibliothek abgelegt werden. Per Drag & Drop zieht sie der Benutzer aus dem Library Explorer in den Report (Abbildung 3). Zunächst empfiehlt es sich, die Datenquelle in einer solchen Bibliothek zu spezifizieren. Ein weiterer Kandidat für die zentrale Pflege sind Data Sets, insbesondere die zur Abfrage von Stammdaten. BIRT bietet derzeit keine automatische Unterstützung für Refactorings, es sollte also vorher klar sein, wie das Projekt aufgebaut ist. Ein exemplarischer Report hilft beim Erstellen des gewünschten Layouts. Folgender Codeausschnitt zeigt den Import des gesamten Report-Kopfes mit Logo und Timestamp, lediglich *Title* wird überschrieben.

```
<grid name="HeaderGrid" extends="GINA.Hdr">
  <overridden-values>
    <ref-entry baseId="9" name="Title">
      <property name="content">
        Mitgliederentwicklung</property>
      <property name="contentType">
        plain</property>
    </ref-entry>
  </overridden-values>
</grid>
```

Das Vererbungskonzept erlaubt es, generische Elemente in Libraries zu verfrachten und sie beim Import anzupassen, was der Wiederverwendungsrate zugutekommt. Als weitere Modularisierungsvariante darf jedes Element eines BIRT-Reports einen Link zu einem anderen Report enthalten. Über Templates kann man neue Reports automatisch mit den passenden Einstellungen (Library-Importe, Layouts) versehen. Ein Template entsteht auf dieselbe Weise wie ein Report und dient anschließend als Vorlage für neue Reports. Nach dem Kopieren besteht keine Beziehung mehr zwischen Template und Report, Änderungen am Template werden also nicht durchgereicht. Da BIRT in Eclipse eingebunden ist, bietet es zahlreiche Erweiterungspunkte, beispielsweise für eigene Ausgabeformate und Chart-Typen.

Fazit

Die beiden hier vorgestellten Reporting-Werkzeuge unterscheiden sich grundlegend: Während BIRT stark auf SQL und Handarbeit setzt, legt Crystal den Schwerpunkt auf Layout und Generierung. Crystal ist ein mächtiges Werkzeug, dessen Leistungsumfang dieser Artikel lediglich anreißt, Funktionen wie Crosstabs, OLAP-Cubes und andere blieben ganz außen vor. Und der Entwickler erzielt schnell Ergebnisse: Es ist möglich, die Reports ohne Datenbank- und SQL-Kenntnisse zu erstellen. Die gute Vorschau ermöglicht Rapid Prototyping. Bei komplexeren Aufgaben zeigen sich jedoch die Grenzen, denn nicht alles was mit SQL möglich ist, lässt sich mit Crystal auch umsetzen. Zudem schränken die Binärdateien das Versionieren der Reports ein. Das Hauptmanko liegt jedoch in der mangelnden Modularisierbarkeit sowie der daraus resultierenden problematischen Wartung. Daher eignet sich Crystal für den Einsatz in Großprojekten und in größeren Teams nur bedingt. Seine Stärken spielt das Werkzeug bei der Datenvisualisierung und beim Adhoc-Reporting aus.

BIRT wartet mit durchdachten Funktionen auf, die den Anwender in die Lage versetzen, auch komplexe Vorhaben anzugehen. Die Report Libraries erlauben ihm, die Reports in Module aufzuteilen. Da ihm der volle SQL-Umfang zur Verfügung steht, sind ausgefeilte Auswertungen möglich. Zudem gibt es viele Ansatzpunkte für eigene Erweiterungen – etwas individuelle Chart-Typen oder Output-Formate. Verteiltes Arbeiten funktioniert gut, BIRT eignet sich daher für den Einsatz in großen Projekten. Nachteil: Das Erlernen aller potenziellen Möglichkeiten dauert lange. Als Eclipse-basiertes Werkzeug richtet sich BIRT klar an den Entwickler. Seine größte Schwäche liegt derzeit in den wenigen unterstützten Ausgabeformaten. (jd)

JOACHIM NELZ

ist Senior Consultant bei der Logica Deutschland GmbH & Co. KG in Sulzbach a. T.

JURI URBAINCZYK

ist Bereichsleiter beim IT-Beratungshaus Iteratec GmbH in München und Frankfurt.

Literatur

[1] Ruth Heidingsfelder, Samir Mimouh; Pentaho, BIRT und JasperReports im Vergleich; Java Magazin 5/2008

[2] George Peck; Crystal Reports 2008; The Complete Reference; McGraw-Hill 2008





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Vorgriff auf Ruby 2.0: Deutlich schneller

Edelsprachlich

Denny Carl

Wann Ruby 2.0 Realität wird, steht noch nicht fest. Mit der aktuellen Entwicklerversion 1.9 können Programmierer ihre Software aber schon auf die Zukunft vorbereiten.

Die ursprünglich aus Japan stammende und hierzulande lange wenig beachtete dynamische Programmiersprache Ruby hat mit dem Web-Framework Ruby on Rails weltweit immens an Popularität gewonnen. Dementsprechend hoch ist die Erwartungshaltung der wachsenden Community an eine Weiterentwicklung der objektorientierten Sprache. Die Version 1.9 gibt mit ihren vielen Änderungen und Verbesserungen einen Ausblick auf die nächste Ruby-Generation.

1993 begann Yukihiro Matsumoto mit seinen Arbeiten an einer Programmiersprache, da er damals vorherrschende wie Perl oder Lisp als unzulänglich empfand. Bei dem Entwurf von Ruby sollten deren Fehler nicht mehr in Erscheinung treten und nur die brauchbaren Eigenschaften vereint werden. Weihnachten 1995 erschien Ruby 0.95. Fast exakt zwölf Jahre später stellte der meist nur Matz genannte Erfinder von Ruby Version 1.9 vor, die einen neuen Meilenstein in der Ruby-Entwicklung einleitet. Sie gilt mehr als Experimentierfeld und soll keinesfalls die aktuell als stabil gekennzeichnete und für den Produktiveinsatz vorgesehene Version 1.8.7 ablösen. Das soll Ruby 2.0 vorbehalten bleiben, dessen Erscheinungsdatum jedoch noch nicht feststeht. Ruby 1.9, von Matz Bleeding Edge genannt, bietet jedoch die Gelegenheit, eigene Programme und Bibliotheken auf Ruby 2.0 und dessen zu erwartenden Neuerungen vorzubereiten.

Besser: Performance und Design

Bei der Entwicklung von Ruby 1.9 galt es, drei Hauptziele umzusetzen: Performance-Verbesserung, Steigerung der Leistungsfähigkeit der Sprache und die Korrektur von Designfehlern beim Entwurf von Ruby.

Ruby-on-Rails-Entwickler bemängeln des Öfteren die fehlende Performance der Sprache, insbesondere beim Einsatz des Frameworks auf Websites mit großen Zugriffsraten. Ruby 1.9 hat in ersten Tests eine in Teilen bis zu 50-fach höhere Geschwindigkeit gezeigt. Ganze Anwendungen konnten laut Entwicklerangaben bis zu zehnmal schneller ausgeführt werden. War die Ruby-Implementierung auf der virtuellen Maschine von Java (JRuby) bisher schneller als Ruby 1.8, so überholt Ruby 1.9 nun diese.

Die Leistungsfähigkeit der Sprache hat das Hinzufügen neuer Eigenschaften sowie die Aufnahme von bisher externen Funktionen in den Ruby-Core erhöht. Unsaubere Sprachkonstrukte haben die Entwickler beseitigt oder korrigiert. Dies führte allerdings dazu, dass Ruby 1.9 zu Vorgängerversionen nicht vollständig kompatibel ist.

Wichtige Inkompatibilitäten

Mit Ruby 1.9 sind Blockparameter grundsätzlich lokale Variablen. Die Verwendung außerhalb des Blocks existierender Objekte als Blockparameter ist nicht mehr möglich.

```
# Ruby 1.8.7
a = 10
2.times { |a| a = 2}
a # => 2
# Ruby 1.9
a = 10
2.times { |a| a = 2}
a # => 10
```

Eine weitere bedeutsame Neuerung taucht in der *String*-Klasse auf. Sie ist kein Enumerable mehr, sondern besitzt auf Zeichenketten zugeschnittene, eigene Iteratoren wie *String#each_char*, *String#each_byte* und *String#each_line* statt nur *String#each*.

Darüber hinaus verarbeitet Ruby Strings nicht mehr als Byte-, sondern als echte Zeichenketten. Dementsprechend gibt der Zugriff auf ein Zeichen über dessen Index nicht mehr den ASCII-Wert, sondern das Zeichen selbst zurück.

Mit dieser Änderung einher geht die längst überfällige Unterstützung von Encodings und Unicode. Über die aus Python bekannten Magic Comments kann ein Programmierer ein Skript so einstellen, dass es ASCII-8BIT (Stan-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

dard), UTF-8, EUC-JP oder viele andere Zeichenstandards verwendet – nun versteht Ruby Japanisch.

```
# Ruby 1.8.7
"Zeichenkette"[0] # => 90
# Ruby 1.9
"Zeichenkette"[0] # => "Z"
"Zeichenkette".encoding # => 
                    #<Encoding:ASCII-8BIT>
```

Weitere Neuerungen

Klassenvariablen behandelt Ruby 1.9 anders. Eine Unterklasse kann den Wert einer Klassenvariablen lesen. Bei deren Veränderung wird jedoch eine lokale Kopie in der Unterklasse erzeugt. Der Wert der Klassenvariablen in der Superklasse bleibt unverändert.

Optionale Parameter einer Methode müssen nun nicht mehr zwingend am Ende der Parameterliste stehen, obwohl dies sicherlich gewöhnungsbedürftig sein dürfte.

```
def test(a, b=2, c)
  puts "#{a}, #{b}, #{c}"
end
test 5,6 # => "5, 2, 6"
test 5,6,7 # => "5, 6, 7"
```

Ein großes Ärgernis stellt bisher bisweilen die Tatsache dar, dass sich die bei der Erzeugung festgelegte Reihenfolge von Hash-Elementen unvorhersehbar verändern kann. Mit Ruby 1.9 ist das Geschichte.

```
h = {:a => 1, :b => 2, :c => 3}
h[:d] = 4
# Ruby 1.8.7
h.values # => [1, 3, 2, 4]
# Ruby 1.9
h.values # => [1, 2, 3, 4]
```

Ruby 1.9 spendiert Entwicklern einige alternative Formen der Notation. So kann man ein Lambda nun mit „->“ notieren. Die Schlüssel-Wert-Paare eines Hashes kann man nun auch durch einen Doppelpunkt trennen.

Onlinequellen

Ruby 1.9 Development Release
www.ruby-lang.org/en/news/2007/12/25/ruby-1-9-0-released/

Changes in Ruby 1.9
eigenclass.org/hiki.rb?Changes+in+Ruby+1.9

Hinweise zur Portierung auf Ruby 1.9
blog.grayproductions.net/articles/getting_code_ready_for_ruby_19

Bei Verwendung von Iterator-Methoden wie *times* oder *each* ohne Block erzeugt Ruby daraus ein Enumerator-Objekt, das beispielsweise später verwendet werden kann. Es handelt sich um sogenannte externe Iteratoren.

Rake, YARV, Oniguruma

Offiziell ist Rake jetzt das Ruby-Build-Tool; bisher musste es jeder eigenständig installieren. Gleiches gilt für den komfortablen Paketmanager Rubygems.

YARV steht für Yet Another Ruby Virtual Machine und bezeichnet eine der größten Neuerungen: eine virtuelle Maschine, die aus Ruby erzeugten Bytecode interpretiert und somit für Verbesserungen in der Geschwindigkeit von Skripten sorgt. Diese VM existierte neben anderen schon eigenständig vor Ruby 1.9. Matz wählte YARV als die für Ruby geeignetste offiziell aus.

Echte, native Threads und damit parallele Prozesse werden mit Ruby 1.9 allmählich Wirklichkeit, obwohl es hier bislang noch Schwierigkeiten gibt.

Hinter Onigoruma steckt eine der mächtigsten Bibliotheken für reguläre Ausdrücke. Matz will sie allem Anschein nach offiziell in Ruby integrieren. JSON for Ruby ist ebenfalls fester Bestandteil der Sprache geworden und ermöglicht somit, es als Alternative für YAML als Format serialisierter Daten zu nutzen.

Fazit

Ruby 1.9 gilt als Zwischenschritt auf dem Weg zur Version 2.0. Vieles befindet sich im Umbruch und ist daher mit Vorsicht zu genießen. Ruby 2.0 soll Ergebnisse des hier nur in Auszügen Vorgestellten enthalten und nach Aussagen von Matsumoto darüber hinaus großen Wert auf Skalierbarkeit von Programmen, Daten und Entwicklerteams legen.

Version 1.9 ist spannend für alle, die den Prozess der Fortentwicklung einer inzwischen bedeutenden Programmiersprache aktiv oder passiv begleiten wollen, die auf die zu erwartenden Features der Zukunft gespannt sind oder ihre eigene Software an die neuen Features anpassen möchten. (hb)

DENNY CARL

ist seit 2001 selbstständiger Webdesigner und -entwickler in Berlin.





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Telepräsenz-Systeme von Tandberg und Cisco

An einem Tisch

Dieter Michel



Wer zeitaufwendige Flugreisen verabscheut oder Energie sparen möchte, kann seine Gesprächspartner aus aller Welt über ein sogenanntes Telepräsenz-System auch an den eigenen Konferenztisch holen. Der Vergleich zweier Systeme dokumentiert zugleich den Stand der Technik.

Mittendrin statt nur dabei", „So nah, als wär man da" – das sind Slogans, die man aus dem Sport- oder Mobilfunkumfeld kennt. Sie würden allerdings gut auf die aktuellen Entwicklungen im Videokonferenzbereich passen, die man unter dem Begriff Telepräsenz (neuhochdeutsch: Telepresence) zusammenfassen kann.

Solche Systeme versuchen dem Anwender das Gefühl zu geben, mit seinen Gesprächspartnern im selben Raum zu sitzen. Dazu gehört deutlich mehr als eine halbwegs störungsfreie Bewegtbild-Übertragung. Die Systeme arbeiten mit großen, HD-tauglichen Flachdisplays, leistungsfähigen Codecs und einer Übertragungskapazität, die eine realistische Bildübertragung zulässt. Insbesondere ist aber der Konferenztisch und der Videokonferenzraum in das Konzept eingebunden, ja er bildet sogar den Schlüssel für die Realitätsnähe der gesamten Installation. *iX* hat sich zwei Systeme angeschaut, die bereits am Markt verfügbar sind: das Experia System von Tandberg in Ratingen und das Telepresence 3000 System von Cisco in Düsseldorf.

Bei Telepräsenz geht es nicht einfach darum, eine Art etwas schickeres Videokonferenzsystem zu bauen, sondern vielmehr darum, die Nutzungsqualität einer Videokonferenz so zu erhöhen, dass sie einer Besprechung mit echten Personen (Face-to-Face-Kommunikation) möglichst nahekommt.

Das ist insofern wichtig, als es für den Einsatz von Videokonferenzen, speziell in Großunternehmen, ganz handfeste Gründe gibt – zu nennen wären etwa die Einsparung von Reisekosten und „toter" Arbeitszeit, die Mitarbeiter durch nicht anderweitig nutzbare Warte- oder Reisezeiten verbringen. Dazu kommen Umweltargumente wie das Einsparen von Treibstoffen und geringere CO_2-Belastung der Umwelt – Punkte, die angesichts steigender Energiepreise einen handfesten wirtschaftlichen Hintergrund bekommen.

Die Akzeptanz von – allgemein gesprochen – Techniken wie Telefon- und Videokonferenzen steht und fällt jedoch zum einen mit dem Einarbeitungs- und Bedienaufwand, zum anderen mit der Nutzungseffizienz. Hierfür gilt also dasselbe wie für die Einführung neuer Software im Unternehmen: Ein neues System mit geänderter Bedienung und Arbeitsweise muss in einem bestimmten Maß zu den Mitarbeitern des Unternehmens passen, sonst wird sie nicht akzeptiert und in der Folge auch nicht im erwünschten Maße genutzt.

Die Illusion des Meetings

Für Videokonferenzen heißt das: Die Übertragung eines Bewegtbildes – im einfachsten Fall mit einer Webcam auf dem eigenen Computermonitor – mag besser sein als eine reine Audioverbindung. Allerdings müssen Mitarbeiter den Umgang mit einem neuen Medium erlernen. Soll man produktiv mit einem solchen neuen System arbeiten, muss aber auch die sogenannte Usability, also die Benutzbarkeit beziehungsweise Benutzerfreundlichkeit stimmen. Aus Sicht der Teilnehmer sollte eine als Videokonferenz angesetzte Besprechung nach Möglichkeit genauso ablaufen wie

iX-TRACT

- Telepräsenz-Systeme ersparen lange Flugreisen zu firmeninternen Besprechungen und vermitteln dem Anwender dennoch das Gefühl, mit seinen über die Kontinente verstreuten Gesprächspartnern im selben Raum zu sitzen.
- Dazu sind vor allem große, HD-taugliche Flachdisplays, leistungsfähige Codecs und eine Standleitung nötig, die eine realistische Bildübertragung zulässt.
- Den Schlüssel zur gelungenen Illusion bildet das Zusammenspiel von Konferenztisch, Raumdesign samt Beleuchtung sowie den Kamera- und Lautsprecherpositionen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

eine Besprechung im eigenen Hause – als hätten eben die anderen die Reise auf sich genommen.

Es gibt Besprechungen, etwa mit potenziellen Neukunden und wichtigen Vertragspartnern, zu denen man persönlich erscheinen muss – auch, um zum Beispiel das Umfeld des Gegenübers besser kennenzulernen oder sich einen Eindruck von den dortigen Betriebsbedingungen zu verschaffen. Ebenso gibt es aber Besprechungen, die regelmäßig stattfinden, bei denen man bestimmte Tagesordnungspunkte abarbeitet, für die eine persönliche Anwesenheit am anderen Standort nicht zwangsläufig erforderlich wäre. Solche Besprechungen gehören zur Routinearbeit, und die beteiligten Personen würden die standortübergreifenden Konferenzen gern ebenso schnell abwickeln wie die hausinternen. Vor allem in großen, international agierenden Unternehmen sind Besprechungen mit Kolleginnen und Kollegen an anderen Standorten, in anderen Ländern und auf anderen Kontinenten an der Tagesordnung.

Das ist mithilfe von Videokonferenz- und Telepräsenz-Systemen möglich, erfordert aber einen hohen Grad der Einbettung des Systems in die betriebsinterne Termin- und Ressourcenplanung sowie eben die Benutzerfreundlichkeit des Systems. Ziel eines optimalen Telepräsenz-Systems ist es, dass die Teilnehmer einen Termin für die Konferenz über ihr übliches Terminplanungssystem vereinbaren, den Konferenzraum als Ressource buchen, die anderen Teilnehmer einladen und sich die Teilnahme bestätigen lassen. Zum Zeitpunkt der Konferenz geht man dann in den gebuchten Videokonferenzraum, und die anderen Teilnehmer sind entweder schon „da“ oder „treffen gerade ein“. Dass, angestoßen von der Terminplanung, das Konferenzsystem rechtzeitig zum Termin entweder eine Point-to-Point-Verbindung (eine Gegenstelle) oder eine Multipoint-Verbindung (mehrere Gegenstellen) zu den anderen Systemen aufbaut, sollte im Idealfall keine Interaktionen der Konferenzteilnehmer mehr erfordern.

Alle an einem Tisch

Eine der Herausforderungen an ein Telepräsenz-System besteht darin, einen überzeugenden Eindruck einer gemeinsamen Besprechung mit Teilnehmern, die sich in einem Raum befinden, zu erzeugen. In diesem Fall vergessen die Teilnehmer recht schnell, dass sie sich in einer technisch vermittelten Gesprächssituation befinden, und können sich voll auf ihre Besprechung konzentrieren.



Komplett integriert: Nicht nur in Düsseldorf sind die Monitore bei Ciscos Telepresence 3000 System in den Konferenztisch integriert. Die drei Kameras befinden sich im Rahmen des mittleren Monitors, die Grenzflächenmikrofone sind in die Tische eingebaut. Mit dem Unified IP-Telefon lassen sich die Verbindungen aufbauen (Abb. 1).

Auf den ersten Blick wirken die Systeme sehr ähnlich und weisen in der Tat eine ganze Reihe gemeinsamer Merkmale auf – eine Folge der gleichartigen Zielsetzung. Ein wichtiges gemeinsames Architekturmerkmal sind der Konferenzraum und seine Möblierung. Um die Illusion eines gemeinsamen Zusammensitzens an einem Tisch zu schaffen, muss eben dieser Tisch samt seiner Umgebung lokal und an den Gegenstellen möglichst identisch gestaltet sein. Das erreicht man mit Vorgaben hinsichtlich der gewünschten Raumgeometrie und der Farbgebung des Raums sowie darüber hinaus einer gemeinsamen Form und Oberflächengestaltung des Konferenztisches.

Die Telepräsenz-Systeme von Tandberg und Cisco Systems bieten in einem mittelgroßen Raum Platz für jeweils sechs Teilnehmer pro Niederlassung. Denkt man sich den Tisch in den virtuellen Raum fortgesetzt, hat er jeweils einen etwa ovalen Grundriss. Die sechs lokalen Teilnehmer sitzen jeweils an der Längsseite insgesamt drei Großdisplays gegenüber. Auf denen erscheinen je zwei Gesprächsteilnehmer eines entfernten Standortes in Lebensgröße. Kamerapositionen und Aufnahmewinkel sind so gewählt, dass sich der Konferenztisch aus der Sicht der lokalen Teilnehmer jeweils über die Bildschirme hinweg auf der entfernten Seite fortsetzt. Auf diese Weise entsteht eine recht realistische Illusion eines Gemeinsam-am-Tisch-Sitzens.

Bei beiden Systemen sind jeweils zwei Teilnehmern ein Großbildschirm, eine Kamera und ein Mikrofon zugeordnet. Die Grenzflächenmikrofone sind jeweils etwa mittig vor den beiden Teilnehmern in den Konferenztisch eingelassen. Im Prinzip besteht das Telepräsenz-System aus drei parallel laufenden Videokonferenzen, die miteinander verknüpft sind und einer gemeinsamen Steuerung unterliegen. Die Kameras und Bildschirme sind HD-tauglich und liefern bei ausreichender Kapazität der WAN-Verbindungen (ISDN oder IP) eine Bilddarstellung in hoher Qualität, die entscheidend zum Gelingen der Illusion beiträgt.

Blickkontakt erwünscht

Ein wichtiger Punkt bei der Auslegung eines Telepräsenz-Systems mit dem Anspruch an die Herstellung einer realitätsnahen Konferenzsituation (unter gut definierten Bedingungen) sind die Positionen der Kameras, weil sie einen großen Einfluss darauf haben, inwieweit die Gesprächspartner einen natürlichen Blickkontakt miteinander aufnehmen können.

Ausgangspunkt ist die Frage, ob und wie man in einer solchen Telepräsenz-Anordnung einen einigermaßen realistisch wirkenden Augenkontakt zwischen den einzelnen Gesprächspartnern herstellen kann. Mit drei Kameras und drei Displays bei sechs Gesprächspartnern an jedem Ende der Verbindung ist das in idealer Weise nicht möglich, weil man nicht für jede Person einen individuellen Bildschirm und eine eigene

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

– blickabhängig steuerbare – Kamera hat. Bei der Auslegung der Kameras muss man sich also für einen Weg entscheiden, der, je nach Prämisse, den besten Kompromiss darstellt.

Perspektive ist Konzeptsache

Nutzt das Videokonferenzsystem nur einen Bildschirm, ist die Sache relativ einfach, weil die infrage kommenden Einblickwinkel nicht allzu groß sind: Man positioniert die Kamera mittig oberhalb oder unterhalb des Bildschirms. Bei drei Bildschirmen wird die Sache komplizierter, weil nicht nur die sechs lokalen Teilnehmer unterschiedliche Blickwinkel auf das Bild eines entfernten Teilnehmers haben, sondern umgekehrt dieser ja auch seinen Kopf dreht, um den Blickkontakt zu seinem jeweiligen Gesprächspartner zu suchen.

Hinsichtlich der Handhabung dieser Situation unterscheiden sich die beiden Lösungen von Tandberg und Cisco. Beide nutzen drei Kameras, die jeweils ein Bildsignal für die drei Monitore erzeugen. Bei Tandberg sind die Kameras jeweils oberhalb der Bildschirme angeordnet und erfassen die beiden sich gegenübersitzenden Gesprächspartner. Das Konzept stellt sicher, dass Gesprächsteilnehmer, die sich direkt gegenübersitzen, auch über das Telepräsenz-System einen natürlich wirkenden Blickkontakt haben.

Für Gesprächsteilnehmer, die schräg auf den Bildschirm schauen, also etwa Teilnehmer rechts außen auf den Bildschirm links außen, funktioniert das nur eingeschränkt. Blickt der entfernte Gesprächspartner geradeaus (in die Kamera), ist der Eindruck für den lokalen Teilnehmer natürlich, der entfernte Partner hat aber keinen direkten Blickkontakt. Dreht der den Kopf, um Blickkontakt herzustellen, wirkt es für den lokalen Teilnehmer ein wenig, als schaue der entfernte Teilnehmer etwas an ihm vorbei – immerhin nicht von ihm weg. Dadurch bleibt sichergestellt, dass alle Teilnehmer entweder einen korrekten Blickkontakt aufbauen können oder zumindest in die richtige Richtung sehen und nicht so wirken, als fixierten sie etwas außerhalb der Gesprächsrunde oder schauten einfach aus dem Fenster.

Beim System von Cisco sind alle drei Kameras zentral über dem mittleren Bildschirm montiert, wobei wiederum jede Kamera so ausgerichtet ist, dass sie zwei Gesprächsteilnehmer erfasst. Hier gilt die Regel für die Gesprächsteilnehmer: Immer in die Kamera schauen. Das bewirkt, dass für die lokalen Teilnehmer die entfernten immer wirken, als sähen sie jeden lokalen Teilnehmer direkt an – weil sie geradeaus aus dem Bild heraus blicken. Ein direkter, natürlicher Blickkontakt ist nur für die beiden mittleren Plätze am Konferenztisch gegeben.

Ciscos Telepresence 3000

Das Cisco Telepresence System (CTS) 3000 nutzt für die Wiedergabe der Konferenzsituation drei nebeneinander angeordnete 65"-Plasmabildschirme und eine Beleuchtungseinrichtung, die wie ein Leuchtrahmen um die Displays herum angebracht ist und dadurch – zusammen mit der Raumbeleuchtung – eine diffuse, praktisch schattenfreie Ausleuchtung des Kamerasichtfeldes sicherstellt. Zum System gehört ebenfalls der Konferenztisch mit den integrierten Mikrofonen und Platz für sechs Personen.

Präsentationen und gemeinsam bearbeitete Dokumente projiziert ein unter dem Konferenztisch integrierter Beamer auf eine geräuschdurchlässige Projektionsfläche unterhalb der Plasmabildschirme. Hinter ihr sind die Lautsprecher des Audiosystems installiert, sodass sich automatisch auch ein gewisser auditiver Richtungsbezug auf die Gesprächspartner der Gegenstellen ergibt.

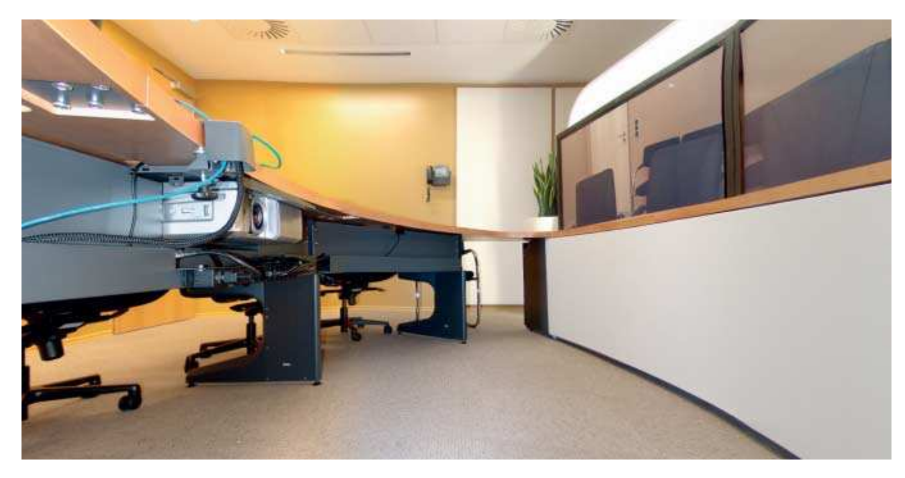
Bei Multipoint-Verbindungen, Konferenzen also mit mehr als einer Gegenstelle, sind nicht mehr alle beteiligten Konferenzteilnehmer gleichzeitig auf den Monitoren darstellbar, weil sonst erstens das Abbild jeder einzelnen Person zu klein wäre und zweitens die Illusion des Gemeinsam-am-Tisch-Sitzens zusammenbräche.

Stattdessen wählten die Entwicklungsingenieure von Cisco eine sprachgesteuerte, paarweise Umschaltung. Dargestellt wird durch Umschalten der Kamerasignale immer diejenige Zwei-Personen-Gruppe der Gegenstelle, von der ein Teilnehmer gerade spricht. Insgesamt kann der Multipoint-Server bis zu 48 Monitore steuern, also 16 CTS-3000-Installationen. Gewöhnen müssen sich die Teilnehmer allerdings daran, dass – um im Bild zu bleiben – die sich gegenübersitzenden Gesprächspartner automatisch ausgetauscht werden, je nachdem, wer gerade spricht.

Einen Durchsatz von 2 bis 5 MBit/s benötigt das CTS 3000 nach Herstellerangaben pro Bildschirm für die Übertragung von Audio- und vor allem Videodaten – abhängig von der gewählten Bildauflösung von 720 oder 1080 Zeilen (progressive). An einer Sitzung sind also drei solcher Datenströme beteiligt, die eigene Codecs herunterrechnen.

Für die Verwaltung der Datenströme sowie der beteiligten Soft- und Hardware ist der Cisco Telepresence Manager zuständig. Er übernimmt außerdem das Veranstaltungsmanagement wie den Verbindungsaufbau und stellt außer einer Helpdesk-Funktion weitere Features wie das gemeinsame Bearbeiten von Dokumenten bereit.

Zur unkomplizierten Einbindung der Telepräsenzanwendung als Ressource in der unternehmensweiten Terminplanung hat Cisco den Telepresence Manager in die vorhandene Unternehmens-Group-



Unterm Tisch: Ein unter dem Konferenztisch angebrachte Beamer projiziert Präsentationen und gemeinsam bearbeitete Dokumente auf die geräuschdurchlässige Leinwand unterhalb des gegenüberliegenden Tisches. Dahinter befinden sich die Lautsprecher (Abb. 2).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ware – bei der ersten Release Microsoft Exchange und Outlook – und in den hauseigenen Unified Callmanager 5.1 integriert. Letzterer ist für den Betrieb des Telepräsenz-Systems erforderlich. Anwender können auf diese Weise Verbindungen auch mit einem Knopfdruck direkt von einem Cisco Unified IP-Telefon aus aufbauen.

Durch Protokolle wie H.264 und SIP (Session Initiation Protocol) sollte das CTS grundsätzlich mit anderen Videokonferenzsystemen kompatibel sein. Sie lassen sich per Gateway (Cisco IPVC) integrieren, der SIP, H.323 und SCCP (Skinny Client Control Protocol) beherrscht. Für die Zukunft stellt Cisco auch eine Kompatibilität mit anderen standardgemäßen Videogeräten mit hoher Auflösung in Aussicht, weist aber darauf hin, dass sein Telepresence als Meeting-Lösung mit Mehrkanal-Audio und -Video arbeitet und daher eine grundsätzlich andere Technik als Videokonferenztechnik mit niedriger Bitrate und einem einzelnen Datenstrom darstellt. Der Schwerpunkt liege daher in erster Linie darauf, den Anwendern ein möglichst realitätsnahes Erlebnis persönlicher Begegnung zu vermitteln.

Die Interoperabilität mit konventionellen Videokonferenzsystemen ist daher zunächst für das kleinere CTS 1000 gedacht, da es mit nur einem Codec, einer Kamera und einem Display arbeitet und mithin konventionellen Videokonferenzsystemen ähnlicher ist.

Tandbergs Experia

Experia nennt Tandberg seine integrierte Telepräsenz-Lösung. Sie basiert auf einem freistehenden Aufbau aus insgesamt vier 50"-Plasmabildschirmen. Davon sind drei nebeneinander angeordnet und dienen zur Wiedergabe der Gesprächspartner. Der vierte (im Tandberg-Jargon: Kooperationsmonitor) ist unterhalb des mittleren Displays installiert und dient der Darstellung von Präsentationen beziehungsweise gemeinsam bearbeiteten Dokumenten. Das Experia-System nutzt mehrere Audio- und Videodatenströme, um die Darstellung der Gesprächspartner in HD-Qualität von 720p oder 1080p zu ermöglichen. Dafür kommen insgesamt vier Codecs vom Typ Tandberg 6000 MXP zum Einsatz.

In Ratingen arbeitet das System mit 2 MBit/s pro Bildschirm und liefert eine sehr realistische Darstellungsqualität. Das Datenblatt spricht von einem Durchsatzbedarf von 8 MBit/s für das Gesamtsystem. Um eine realistische Illusion einer gemeinsamen Gesprächsrunde zu gewährleisten, nutzt auch Tandberg einen vorgefertigten Konferenztisch und eine weitgehend vordefinierte Gestaltung des Raums, sodass das Abbild der Gegenstelle wie eine virtuelle Fortsetzung des realen Raums wirkt.

Die Gesprächsteilnehmer sitzen sich je Bildschirm paarweise gegenüber. Wie bereits erwähnt, nutzt das Experia-System eine Kameraanordnung, bei der sich gegenübersitzende Teilnehmer einen korrekten Blickkontakt aufbauen können. Je zwei Personen teilen sich ein im Tisch installiertes Grenzflächenmikrofon. Die Lautsprecher unter den seitlichen Bildschirmen erlauben eine einigermaßen richtungsgetreue auditive Lokalisierung der Gesprächspartner.



Freistehend: Tandbergs Experia System arbeitet, wie hier in der Niederlassung Ratingen, mit einer separaten Videowand. In ihr sind ein vierter Monitor für Dokumente und Präsentationen, die Kameras und die Lautsprecher integriert (Abb. 3).

Für Multipoint-Verbindungen von bis zu vier Standorten beherrscht das System mehrere Modi. Einer davon erweitert die Gesprächsrunde auf vier Personen pro Standort und Monitor. Dafür schaltet das System auf eine vierte Kamera um, die den zentralen Bereich des Konferenztisches mit insgesamt vier Personen erfasst. Bildwinkel und Perspektive der Kamera sind so gewählt, dass sich zusammen mit der Geometrie des Konferenztisches eine fast nahtlos über alle drei Bildschirme laufende Gesamtansicht der drei Gegenstellen mit je vier Teilnehmern ergibt. Es entsteht der Eindruck, als säße man nun an einem vergrößerten Konferenztisch zusammen. Den Kompromiss, nur vier Teilnehmer zu erfassen, wählten die Entwickler, um den einzelnen Teilnehmer nicht zu klein wirken zu lassen. Sollte es notwendig sein, Konferenzen mit jeweils sechs Teilnehmern an jedem Standort zu führen, beherrscht das System zudem die sprachgesteuerte Umschaltung.

Tandberg weist darauf hin, dass das Experia-System auf gängigen Videokonferenzstandards wie H.261, H.263, H.263+, H.263++ (Natural Video), H.264 und H.264RCDO aufsetzt, also keine proprietären Protokolle und Codecs benutzt. Der Tandberg-6000-MXP-Codec ermöglicht auch eine Interoperabilität mit Standard-H.323-Videokonferenzsystemen, gegebenenfalls mit Qualitätsabstrichen entsprechend den Leistungsmerkmalen der Gegenstelle. Die Illusion, mit den Gesprächspartnern gemeinsam am selben Ort zu sein, stellt sich nur ein, wenn die Gegenstelle mit einem entsprechenden Telepräsenz-System arbeitet.

Zur Bedienung des Experia-Systems dient ein drahtlos angebundenes Touch Panel. Darüber hinaus können die Teilnehmer die Zuspielquellen für Präsentationen über Sensortasten steuern, die in den Tisch integriert sind. Die Zeitplanung und den automatisierten Auf- und Abbau von Sitzungen kann man auch den unternehmenseigenen Termin- und Ressourcenplanungs-Systemen wie Outlook oder Lotus Notes überlassen.

Zusammenfassung

Tandberg und Cisco-Systems stellen mit ihren neuen Telepräsenz-Systemen eine neue Generation von Videokonferenzlösungen vor, die über eine reine Ton- und Bewegtbild-Übertragung zwischen den Gegenstellen deutlich hin-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ausgeht. Das Ziel beider Konzepte ist es, den Konferenzteilnehmern möglichst realitätsnah den Eindruck zu vermitteln, mit ihren Gesprächspartnern im selben Raum zu sitzen, selbst wenn bis zu vier über den ganzen Globus verteilte Standorte an der Telepräsenz-Konferenz beteiligt sind. Zu diesem Zweck verbinden sie modernste Audio- und Videotechnik wie Bildschirme in HD-Auflösung, leistungsfähige Codecs, hohe Bandbreite für hohe Bildfrequenz und hohe Auflösung mit einer ausgeklügelten Kombination aus Konferenztischgestaltung, Kamerapositionen und Raumdesign.

In einer Konferenz mit einem solchen System vergisst man schon nach kurzer Zeit, dass man es nicht mit persönlich anwesenden Gesprächspartnern zu tun hat. Zusammen mit der wichtigen Integration eines solchen Systems in die unternehmenseigene Termin- und Ressourcenplanung kommen die Telepräsenz-Systeme dem Ziel bereits sehr nahe, regelmäßige Besprechungen mit entfernten Standorten fast wie in einer Face-to-Face-Kommunikation abzuwickeln, ohne sich mit dem Zeit- und Kostenaufwand für regelmäßige (Fern-) Reisen zu belasten. Dass eine solche Arbeitsweise wegen verminderten Treibstoffverbrauchs und CO_2-Ausstoßes auch Vorteile für die Umwelt bietet, liegt auf der Hand.

Beide Systeme sind als Komplettlösungen konzipiert. Bei der Einführung im Unternehmen sollte man schon wegen des nicht geringen Preises – Cisco verlangt 300 000 Euro pro Standort, Tandberg 250 000 Euro – eine kompetente Fachberatung mit einplanen. (sun)



Große Runde: Bei einer Multipoint-Konferenz kann das System die Runde auf insgesamt 16 Teilnehmer erweitern. Dazu schaltet es auf die vierte Kamera um, die die mittleren vier Teilnehmer am Tisch erfasst (Abb. 4).

DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



CakePHP 1.2 mit Unicode und Paginierung

Aus der Bäckerei

Dirk Ammelburger, Robert Scherer

Was Rails für Ruby ist, sollen verschiedene Frameworks für PHP ebenfalls erreichen: Webanwendungen nach dem Model-View-Control-Muster zu erstellen. Eins von ihnen, CakePHP, kommt jetzt in einer neuen Version.

Vor gut einem Jahr hat *iX* verschiedene PHP-Frameworks unter die Lupe genommen [1] – darunter CakePHP. Anfang August sollte es in der Version 1.2 mit signifikanten Neuerungen und Verbesserungen gegenüber dem Vorgänger 1.1 freigegeben sein. Release-Kandidat 2 liegt vor. Der Versionssprung erscheint zwar minimal, birgt aber eine Reihe struktureller Verbesserungen und neuer Features.

CakePHP (cakephp.org), ein 2005 erstmals veröffentlichtes Open-Source-PHP-Framework, nimmt viele Konzepte der Mutter aller Rapid-Development-Frameworks, Ruby on Rails, auf und überführt sie in die Welt von PHP. Allerdings ist CakePHP keine reine Portierung von Rails auf PHP, sondern ein unabhängiges Projekt mit vielen eigenen Features.

Grundlage ist das Model-View-Controller-Pattern (MVC), das die Trennung von Daten, Präsentation und Programmsteuerung vorschreibt und für eine saubere, übersichtliche und wartbare Programmstruktur sorgt. Außerdem hat CakePHP mit Rails gemein: die Prinzipien „Don’t Repeat Yourself“ (DRY) sowie „Convention over Configuration“. Sie beschreiben die Wiederverwendbarkeit von Code für Standardaufgaben und die Vermeidung von Konfigurations-Overhead durch Konventionen hinsichtlich Programmstruktur, Aufbau und Benennung. Das Framework wurde für PHP 5 entwickelt, ist aber durch für PHP 4 nachgebildete Funktionen vollständig abwärtskompatibel.

Um das Framework für den kommerziellen Einsatz tauglich zu machen, haben die Verantwortlichen Ende 2005 die Cake Software Foundation gegründet, die die Organisation und Weiterentwicklung des Projekts betreut, Schulungen für Entwickler vornimmt und Unternehmen die Sicherheit sowie den Qualitätsanspruch einer professionellen Software bietet. CakePHP steht unter der MIT-Lizenz, die es erlaubt, mit ihm nicht-quelloffene Software zu entwickeln und kommerziell zu nutzen – eine wichtige Voraussetzung für den Einsatz in Unternehmen.

Unicode und Internationalisierung

Version 1.2 bringt eine ganze Reihe von Neuerungen mit, die im Prinzip in zwei Kategorien gehören: Auf der einen Seite stehen neue Features, die in der Version 1.1 nicht verfügbar waren; auf der anderen Seite Verbesserungen beziehungsweise Optimierungen bestehender Eigenschaften. Eine der fundamentalen Änderungen, die auf den ersten Blick nicht sofort auffällt, ist die durchgängige Unicode-Unterstützung im Framework – unabhängig von der PHP-Installation. Wenn keine Multibyte-Unterstützung vorhanden ist, werden die Funktionen in nativem PHP nachgebildet.

Diese Änderung ist wesentlich für die Unterstützung der neu hinzugekommenen Möglichkeit der Lokalisierung und Internationalisierung von Anwendungen. Aufgaben wie Mehrsprachigkeit und landesspezifische Formate – oft Kandidaten für Schweißausbrüche bei Entwicklern – lassen sich damit schnell und einfach lösen. Basis dessen ist eine Erweiterung der verwendeten Model-Klassen durch eine solide Implementierung des *gettext*-Standards auf Präsentationsebene und in der Haltung dynamischer Daten in einem DBMS. Eine bestehende Applikation können Entwickler sogar im Nachhinein mit relativ wenig Aufwand in eine mehrsprachige Anwendung umschreiben.

Ein Erkennungsmerkmal vieler Rapid-Development-Frameworks ist die Option automatischer Code-Generierung, wie auch in CakePHP vorhanden. Stichwort Rapid Prototyping: Das Framework erzeugt beim Start die nötigen Quelldateien der schon definierten Datenstruktur folgend beispielsweise in Form einer Datenbanktabelle, um eine komplette Weboberfläche zur Ansicht und Bearbeitung dieser Daten zur Verfügung zu stellen. Bis dahin

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

haben Entwickler noch keine Zeile Quelltext geschrieben. Auf Basis dieses Grundgerüsts entwickeln sie erst danach ihre individuelle Anwendung. Dieses „Baking“ genannte Vorgehen wird über die Konsole gesteuert. Sie bietet kommandozeilenbasierten Zugriff auf eine Anwendung, was sich etwa für Wartungsarbeiten in der Applikation anbietet.

Datenquellen für die Models

Viele Verbesserungen enthält die Model-Schicht in der MVC-Implementierung. So dienen jetzt *DataSources* als Datenquelle für die Models. Letztere kapseln den Zugriff auf die durch *DataSources* bereitgestellten Daten, die beispielsweise in Form einer Datenbanktabelle, einer XML-Datei oder eines Webservice existieren können. Durch diese Struktur stehen die Daten dem Entwickler einheitlich zur Verfügung.

Ein weiteres Feature sind Model-Behaviors, die es erlauben, eine Model-Klasse um bestimmte Funktionen zu erweitern und das bestehende Verhalten beeinflussen. Ein Beispiel dafür ist das mitgelieferte *TreeBehavior*, das eine Standard-Model-Klasse so verändert, dass sie eine „Nested Set“-Baumstruktur darstellen kann.

Auch an der Präsentationsschicht des Frameworks haben die Entwickler kräftig gewerkelt und der aktuellen Version einige Features spendiert. Dazu gehört ein neues System zur einfachen Paginierung, der seitenweisen Darstellung von Daten. Dieses System zieht sich durch alle drei MVC-Schichten und bietet so hohe Flexibilität.

Nützliche Helfer für Entwickler

Im View unterstützen sogenannte Helfer die Arbeit, die immer wiederkehrende Aufgaben stark vereinfachen. Der wohl wichtigste in diesem Framework ist der neu hinzugekommene *FormHelper*. Wichtig deshalb, weil CakePHP meist zur Entwicklung datenbankgestützter Applikationen dient und Formulare in solchen Anwendungen eine zentrale Rolle spielen. Mit dem *FormHelper* lassen sich mit wenigen Zeilen Code Formulare entwickeln und mit Daten befüllen. Durch die Verknüpfung mit dem Model kennt der *FormHelper* die Datentypen der Felder und gibt die dem jeweiligen Datentyp entsprechenden Formularelemente automatisch aus. Darüber hinaus bekommt der *FormHelper* Informationen über eventuelle Validierungsfehler und zeigt sie an.

Gerade im Rapid Development darf die Sicherheit nicht zu kurz kommen. Deshalb gibt das Framework dem Entwickler eine Reihe Werkzeuge an die Hand. Dazu gehört die *SecurityComponent*, die Formulare durch Mechanismen wie das automatische Generieren von Sicherheitsschlüsseln, vor Missbrauch (Spambots) schützt. Ähnliches gilt für die Prävention von Session-Hijacking durch sich ständig ändernde Session-IDs. All das geschieht auf Wunsch automatisch. Für den Schutz vor SQL-Injections sorgt ein robustes Input-Handling, das alle Formulareingaben, bevor es sie an die Applikation übergibt, säubert. Mit der *Sanitize*-Klasse bietet CakePHP ein zusätzliches Werkzeug mit mehr Einfluss auf das Säubern und Kontrollieren von Benutzereingaben.

Authentifizierung und SEO-optimierte URLs

Eine immer wiederkehrende Aufgabe in der Entwicklung von Webanwendungen ist die Zugriffskontrolle. Die *AuthComponent* erlaubt es, ein vollständig funktionsfähiges und anpassbares Authentifizierungssystem in eine Anwendung zu integrieren. Damit entfallen lästige Aufgaben wie das manuelle Abgleichen von Zugangsdaten mit der Datenbank und das Setzen von entsprechenden Session-Einträgen; das geschieht vollständig im Hintergrund. Die Autorisierung von Aktionen kann ebenfalls über die *AuthComponent* aktiviert werden. Hier können Entwickler selbst entscheiden, ob die Autorisierungsstelle ein beliebiges Objekt, ein LDAP-Server oder ein Webservice sein soll. Access Control Lists hat CakePHP ebenfalls implementiert.

Dynamische Anwendungen sind nicht unbedingt suchmaschinenunfreundlich. CakePHP erlaubt es durch das *Routes-System*, saubere URLs mit einer simplen Konfigurationssyntax zu gestalten. Ein REST-konformer Webservice lässt sich so ebenfalls einfach realisieren. Ob es sich um HTML, XML, einen RSS- oder JSON-Feed als Ausgabe handeln soll, ist unerheblich – mit dem sogenannten Resource Type Handling kann der Entwickler den Ausgabetyp durch eine simple URL-Erweiterung, beispielsweise *.rss*, steuern.

Schließlich liefert CakePHP eine Reihe nützlicher Helferlein mit. Dazu gehören eine E-Mail-Komponente, eine Komponente zum Handling von Sessions und Cookies sowie eine einfach zu konfigurierende Caching-Engine, die sowohl Datenbankzugriffe als auch komplette oder nur Teile einer Ausgabe zwischenspeichern.

Eine eigene Test-Suite, die das Unit-Testing-Framework SimpleTest nutzt, enthält das Framework ebenfalls. Auch der CakePHP-Kern ist gut durch Unit-Tests abgedeckt und damit stabil und verlässlich.

iX-Wertung

⊕ Entwicklungsgeschwindigkeit
⊕ Erlernbarkeit
⊕ mitgelieferte Komponenten
⊖ Dokumentation unvollständig
⊖ performanceintensiv

Fazit

Alles in allem handelt es sich bei Cake PHP 1.2 um ein ausgereiftes und solides, aber vor allem einfach zu erlernendes PHP-Framework, das die Entwicklung von Webapplikationen deutlich beschleunigen kann. Wer sich an die empfohlenen Konventionen und Standards hält, dessen Anwendung bleibt gut strukturiert und wartbar. (hb)

DIRK AMMELBURGER UND ROBERT SCHERER

sind freiberufliche Webentwickler in München und Autoren des 2008 bei O’Reilly erschienenen „Webentwicklung mit CakePHP“.

Literatur

[1] Markus Franz; Webprogrammierung; Das nächste Jahrtausend; PHP-Frameworks: Zend, eZ Components, Symfony und CakePHP; *iX* 9/2007, S. 56





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

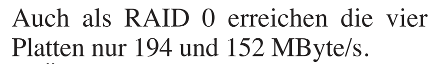
Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Arecas Mini-RAID-Systeme ARC-4020 und ARC-5020 mit eSATA-Anschluss

Rennklötzchen

Michael Riepe



Externe Festplatten und kleine RAIDs mit USB-2.0-Anschluss sind weitverbreitet. Allerdings arbeiten sie deutlich langsamer als interne (S)ATA-Platten. Vor allem für RAID-Systeme eignet sich eSATA erheblich besser.

Nicht jeder benötigt große Speichersysteme mit SAS-, SCSI- oder gar Fibre-Channel-Anschluss. Ein paar Terabyte mehr Speicher bekommt man heute günstiger in Form eines kleinen SATA-RAIDs. Spielt Geschwindigkeit keine große Rolle, genügen Geräte mit USB- oder Firewire-Schnittstelle, die rund 30 MByte/s lesen und schreiben.

Moderne (S)ATA-Festplatten arbeiten erheblich schneller. Sogar für 2,5-Zoll-Platten wird USB 2.0 zum Engpass: Neuere Modelle liefern zwischen 60 und 90 MByte/s. Als Alternative bietet sich eine eSATA-Verbindung an, die die Fähigkeiten der Platte voll ausreizt [1].

iX hat zwei RAID-Systeme von Areca (www.areca.com.tw) unter die Lupe genommen, die davon Gebrauch machen: den ARC-5020 mit vier Platten und integriertem Controller sowie das eSATA-Plattengehäuse ARC-4020 mit separatem RAID-Controller (ARC-1202) für den PCI-Express-Bus (1x). Der ARC-5020 war mit vier Seagate Barracuda ES.2 (ST3500320NS, 500 GByte) bestückt, die anschließend auch im 4020 zum Einsatz kamen.

Konfiguration via Browser

Typisch für Areca-Controller ist, dass sie über eine eigene Ethernet-Schnittstelle zur webbasierten Konfiguration verfügen. Das trifft sowohl auf den RAID-Controller im ARC-5020 zu als auch auf die Steckkarte ARC-1202. Ersterer zeigt auf dem integrierten LC-Display die per DHCP zugeteilte Adresse an; beim ARC-1202 muss der Nutzer sie im Setup oder im Log des DHCP-Servers suchen. Steht kein Ethernet zur Verfügung, lässt sich der ARC-5020 über die serielle Schnittstelle (RS-232, RJ11-Buchse) konfigurieren.

Während der ARC-4020 nur einen eSATA-Anschluss aufweisen kann, lässt sich der ARC-5020 zur Not auch mit USB fahren – allerdings nur im ersten und zweiten Gang (USB 1.1/2.0). Die PCIe-Controller-Karte ARC-1202 besitzt zwei eSATA-Anschlüsse, an die sich sowohl Einzelplatten also auch Plattengehäuse mit Port-Multiplier wie das ARC-4020 anschließen lassen; maximal unterstützt der Controller acht Festplatten. Allerdings muss der Nutzer seinem Rechnergehäuse Gewalt antun, will er beide eSATA-Buchsen nutzen: Die Anschlüsse liegen zu weit auseinander.

Bei den Performance-Messungen kamen wie üblich die *iX*-Storage-Benchmarks *dread* und *dwrite* unter Linux zum Einsatz. Als Testplattform diente ein FSC Esprimo P5600 mit AMD Athlon64 3000+, 1 GByte RAM und SiS-Chipsatz. Zunächst schloss der Tester den ARC-5020 über eine Slotblende an den internen SATA-Controller an. Der ermittelte Durchsatz fiel mit rund 60 MByte/s jedoch mager aus. Am eSATA-Port eines Dawicontrol DC-310e las das RAID-System 86 MByte/s und schrieb 103 MByte/s – immer noch zu wenig, bedenkt man, dass die verwendeten Seagate-Festplatten mit 110 MByte/s arbeiten.

Erst im Pass-through-Modus am ARC-1202 wird der ARC-5020 lebendiger. Konfiguriert man die Platten als RAID 5, liest und schreibt er 191 beziehungsweise 155 MByte/s. RAID 0+1 ist mit 189 und 128 MByte/s trotz des geringeren Rechenaufwands langsamer. Auch als RAID 0 erreichen die vier Platten nur 194 und 152 MByte/s.

Ähnliche Zahlen liefert der ARC-4020 mit dem ARC-1202 als RAID-Controller: 193 und 152 MByte/s für das RAID 5, 194 und 127 MByte/s für das RAID 0+1 sowie 194 und 153 MByte/s fürs RAID 0. Außerdem beherrscht der ARC-1202 noch den RAID-Level 6 (double parity). Der dürfte sich allerdings nur lohnen, wenn man zwei ARC-4020 mit insgesamt acht Platten anschließt.

Fazit

Den ansonsten durchweg positiven Eindruck trübt die Tatsache, dass die Geräte nicht die maximal mögliche Leistung erreichen – der eSATA-Anschluss kann 300 MByte/s übertragen, eine PCI-Express-Lane immerhin 250 MByte/s. Ob dafür die Areca-Controller verantwortlich sind oder der SiS-Chipsatz des Testrechners, ließ sich vor Redaktionsschluss nicht mehr klären. Die miserable Leistung an den anderen Controllern weist allerdings auf den Chipsatz hin.

In Deutschland sind die Geräte für 486,50 (ARC-5020, ohne Platten), 293,20 (ARC-4020) beziehungsweise 200,80 Euro (ARC-1202) bei der Starline Computer GmbH (www.starline.de) erhältlich, die auch die Testgeräte zur Verfügung stellte. (mr)

Literatur

[1] Susanne Nolte; Massenspeicher; Außenstelle; Erste eSATA-Platte samt Controller; *iX* 11/2006, S. 82

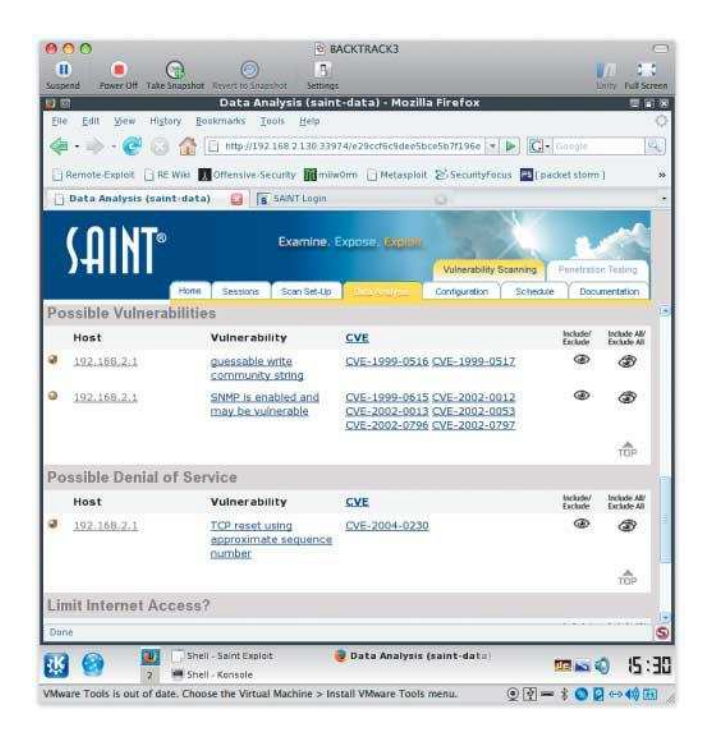




© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Backtrack 3 integriert kommerzielle Werkzeuge

Schein-einbruch

Jörg Riether

Backtrack ist eine auf Einbruchstests spezialisierte Werkzeugsammlung auf einer Linux-Live-CD. Version 3.0 liefert erstmals auch kommerzielle Werkzeuge mit.

In der neuen Backtrack-Version hat sich das Entwicklerteam um die Gründer Max Moser (Schweiz) und Mati Aharoni (Israel) einiges Neues einfallen lassen. Los geht es schon beim Herunterladen: Backtrack 3 [a] steht nämlich nicht wie bisher lediglich als CD- und USB-Image bereit, es gibt jetzt überdies eine bereits vorinstallierte VMware-Version, die in Form eines knapp 700 MByte großen RAR-Archivs daherkommt.

Sie ließ sich sowohl auf einer VMware-Workstation als auch auf der Mac-Variante VMware Fusion ohne Murren ausführen. Der große Vorteil: Diese Variante kann man individuell anpassen und, was noch wichtiger ist, man kann fehlende Software nachträglich installieren.

Nessus und andere Tools nachinstallieren

Für die vorliegende Version erweist sich das neue Feature gleich als notwendig, denn in der Werkzeugsammlung ist wegen geänderter Lizenzbedingungen der bekannte Schwachstellenscanner Nessus nicht enthalten. Das ist kein Versäumnis des Backtrack-Teams, vielmehr verbietet der Nessus-Hersteller Tenable die indirekte Weiterverbreitung. Man muss es sich also direkt von Tenable besorgen, nachdem man sich registriert hat, es ist aber nach wie vor kostenlos erhältlich. Mit einigen Kniffen kann man sich Nessus dann nachträglich im VMware-Image installieren, mehr dazu später.

Erstmals sind kommerzielle Tools in Backtrack integriert, denn dem Entwickler Mati Aharoni gelang es, spezielle Lizenzabkommen mit den Herstellern Saint und Maltego zu treffen. Bei Saint (siehe Aufmacher) handelt es sich um ein kombiniertes Spezialwerkzeug des gleichnamigen Herstellers, das ähnlich wie Nessus nach bekannten Schwachstellen suchen kann. Darüber hinaus kann es allerdings auch die gefundenen Schwachstellen, vergleichbar dem Werkzeug Metasploit [2], aktiv ausnutzen. Und das Ganze derart komfortabel, dass selbst ein Laie sofort damit arbeiten kann.

Saint stellt für alle Backtrack-Benutzer eine spezielle einjährig gültige Lizenz aus: Eine einfache Mail an Saint (sales@saintcorporation.com) mit der Information, man sei Backtrack-Benutzer und wolle die versprochene Lizenz, genügte. Ungefähr zwei Stunden später lag die Lizenz im Posteingang und ließ sich ohne Fehler in Saint einbinden.

Maltego, kommerzielles Werkzeug Nummer zwei in der Backtrack-Toolkiste, ist ein universeller forensischer Datensammler für Netzwerke. Er kann die gesammelten Daten grafisch übersichtlich aufbereiten und die Ergebnisse dynamisch darstellen. Das heißt, verschiedene Auswertungen lassen sich kombinieren, Maltego findet automatisch die Gemeinsamkeiten und stellt sie ebenfalls übersichtlich dar.

Kein Sparzwang bei Werkzeugen

Besonders bei großen Netzwerken oder -strukturen im Internet punktet Maltego durch die grafische Aufbereitung und seine intuitive Bedienbarkeit. Backtrack 3 enthält die „Community Edition“, die gegenüber der Vollversion nur wenig, zum Beispiel in der Analyse einer Mehrfachmarkierung, eingeschränkt ist.

Onlinequellen

[a] Backtrack 3	www.remote-exploit.org/backtrack.html
[b] Wiki	wiki.remote-exploit.org/index.php/Main_Page
[c] Forum	forums.remote-exploit.org
[d] Download	www.remote-exploit.org/backtrack_download.html
[e] Saint	www.saintcorporation.com
[f] Maltego	www.paterva.com/maltego
[g] Fast-Track	www.securestate.com/Pages/Fast-Track.aspx
[h] Karma	www.theta44.org/karma
[i] Anleitung für die Nessus-Installation	www.riether.com/2008/07/installing-nessus-on-backtrack-3.html

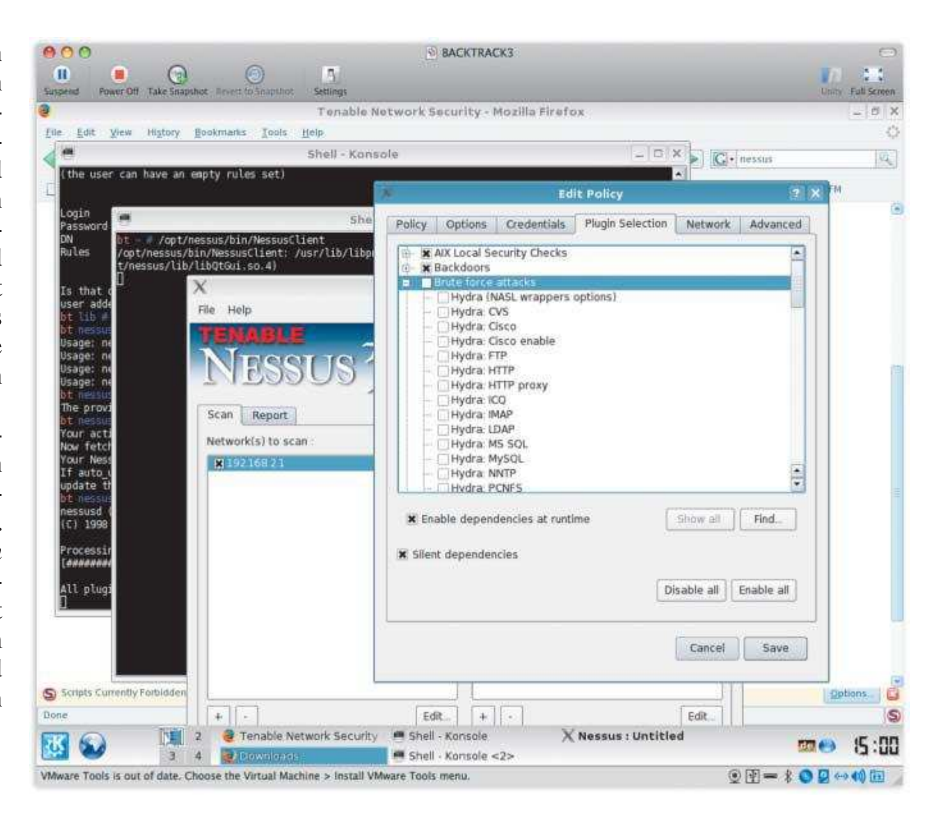
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Die Integration der kommerziellen Tools bedeutet jedoch keinesfalls den Verzicht auf das alte Backtrack-Inventar, ganz im Gegenteil. Alte Backtrack-Hasen finden sich schnell zurecht und fast alles ist am gleichen Platz wie in der Vorgängerversion, auch Spezialtools wie Metasploit – in Version 2 und 3 koexistent vorhanden – sind nicht dem Rotstift zum Opfer gefallen. Dies gilt ebenso für die zahlreichen für die sogenannte Packet Injection gepatchten WLAN-Treiber.

Größere Wörterbücher, Sammlungen et cetera finden sich nicht mehr in Backtrack, lediglich vereinzelt in Programmordnern von Brute-Force-Tools. Dafür liefert die CD aber mit *crunch* einen leistungsfähigen Wörterbuch-Generator. Im WLAN-Bereich kam mit *spoonwep* ein Werkzeug dazu, mit dem sich die WEP-Verschlüsselung (Wired Equivalent Privacy) besonders einfach brechen lässt.



Endlich komplett – mit einigen Kniffen kann man den Schwachstellenscanner Nessus nachinstallieren (Abb. 1).

Für Laien bedienbar

David Kennedys Python-Skripte, die unter dem Namen *fast-track* zusammengefasst sind, bilden eine Kontrollzentrale für Penetrationstests aller Art. Selbst Laien in diesem Bereich können das Werkzeug bedienen – sie müssen lediglich *./fast-track -g* aufrufen und finden ein komfortables Web-Interface vor. Besonders die bekannten Metasploit-*autopwn*-Funktionen, die ein Netz automatisch auf Schwachstellen untersuchen, gewinnen dadurch an Komfort. Erfahrenen Testern seien die Optionen *-i* oder *-c* ans Herz gelegt, damit erreicht man die interaktive beziehungsweise die Kommandozeilen-Version.

Backtrack 3 enthält eine speziell modifizierte Skriptsammlung, die auf dem Metasploit-Framework und der Sicherheitswerkzeugsammlung Karma [h] für Wireless Clients beruht, und erhält damit eine neue Qualität im Bereich WLAN-Penetrationstests. Man kann mit diesen Skripten, vereinfacht gesagt, einen Access Point fälschen, der dann, gespickt mit multiplen Abfangmechanismen, als Man-in-the-Middle fungieren kann.

Hinter Karma verbirgt sich eine interessante Technik: Ursprünglich handelte es sich um einen Patch für den Linux-MADWifi-Treiber, mit dessen Hilfe man einen speziellen Access Point erschaffen kann, der auf jede angefragte SSID (Service Set Identifier) korrekt antwortet – ergo werden sich bei einem etwaigen Einsatz möglicherweise zahlreiche WLAN-Clients direkt mit einem Karma-System verbinden wollen. Die Sicherheitsauditorin oder ihr Kollege sollte sehr genau wissen, was sie tut, bevor sie Karma einsetzt.

Wer auf Nessus nicht verzichten möchte, sollte die vorinstallierte VMware-Version von Backtrack 3 nutzen. Man kann für den Nessus-Client und -Server auf die Softwarepaket-Archive Fedora Core 8 RPMs von der Tenable-Homepage zurückgreifen. Man wandelt sie zunächst mit dem Werkzeug *rpm2tgz* in tgz-Dateien um und startet danach einfach das *slackware pkgtool*. Nach einigen manuellen Konfigurationsschritten läuft Nessus einwandfrei (Anleitung unter [i]).



Daten und iX-Wertung

Backtrack

Live-CD mit Einbruchstest-Werkzeugen

Entwickler: Max Moser, Mati Aharoni

⊕ mächtige kommerzielle Tools

⊕ auch als VMware-Image vorhanden

⊕ breite Hardware-Unterstützung

Fazit

Ursprünglich entstanden durch die Fusion aus Whoppix/Whax und Auditor stellt Backtrack heute einen Quasistandard für eine umfassende Sammlung von Tools für Penetrationstests aller Art dar, und das zum Nulltarif. Durch seine Vielfalt, den Funktionsreichtum und die einfache Benutzbarkeit ist Backtrack zum aktuellen Zeitpunkt praktisch konkurrenzlos. (ur)

JÖRG RIETHER

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisierung. Er arbeitet als Abteilungsleiter der EDV bei der Zentrum für Soziale Psychiatrie Haina gGmbH.

Literatur

[1] Jörg Riether; Penetrationstests; Versuchter Einbruch; Backtrack 2.0: Attacke „out of the box“; *iX* 5/2007, S. 78

[2] Jörg Riether; Security; Gefährliche Experimente; Metasploit 3.1; *iX* 6/2008, S. 74





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



KVM mit DVI-Anschluss
für zwei Monitore und acht Rechner

Achtfache Kontrolle

Ralph Hülsenbusch

Grund für den ungebrochenen Trend zum Zweitmonitor ist der Wunsch nach größeren Darstellungsflächen. Wer zudem mehr als einen Rechner im Blick haben möchte, greift zu einem KVM-Umschalter. Beides zu können, hat Guntermann & Drunck mit Mehrkanal-KVMs verwirklicht.

Administratoren brauchen Weitblick, vor allem an ihrem Arbeitsplatz, geht es doch darum, in der Regel mehrere Server oder Workstations zu überwachen. Ähnliches gilt für Anwender, die mehrere Rechner gleichzeitig nutzen wollen, etwa um die Börsenkurse unter die Lupe zu nehmen. Große Monitore, am besten mehrere, sind eine willkommene Hilfe, und dem Stand der heutigen Technik folgend sollten LCDs am Digital Visual Interface (DVI) ohne analoge Umwege anschließbar sein. Solchen Bedürfnissen kommt die Guntermann & Drunck GmbH (G & D) im siegerländischen Wilnsdorf mit ihrem Switch für Keyboard, Video und Maus (KVM) vom Typ DVIMUX entgegen.

Das Gerät gibt es entweder in PS2- oder in USB-Ausführung, das gemeinsam mit den Videosignalen je einen Audioeingang und -ausgang umschaltet. Im Unterschied zu herkömmlichen KVMs kann ein DVIMUX digitale Videosignale übertragen. G & D verwendet dazu die üblichen DVI-Buchsen, die das analoge Signal mit durchreichen. Der Hersteller gibt für die analoge Grafikdarstellung eine maximale Auflösung von 1920 × 1440 bei 75 Hz an, für die digitale 640 × 480 bei 100 Hz bis zu 1920 × 1200 bei 60 Hz. Die Übertragungsfrequenz beträgt 400 MHz. Die KVMs tragen ein schickes Alukleid, das den Schreibtisch nicht verschandelt, das Material zum Einbau in ein 19-Zoll-Rack liegt bei. Es gibt Varianten zur Ansteuerung für 2, 4 und 8 Rechner, die beiden letztgenannten als Multi-Channel-Version, bei der man mehrere Monitore anschließen kann.

Für vier Rechner genügen 270 mm Gehäusebreite, der Achtfachumschalter braucht 435 mm Platz in der Breite. DVIMUX4 ist für zwei, drei und vier Monitore lieferbar, DVIMUX8 nur für zwei (MC2). Bei den DVI-Monitorkabeln empfiehlt G & D eine maximale Länge der Kabel von 5 m. Bei größeren Entfernungen sollten Anwender zu aktiven DVI-Kabeln greifen, die Guntermann & Drunck ebenfalls im Programm hat.

Buchsen-Phalanx hinter schlichter Front

Ins Labor kam der DVIMUX8-MC2 mit USB-Anschlüssen für Keyboard und Maus. Die Rückseite belegen die acht mal fünf Anschlüsse für die zu bedienenden Rechner: je zwei DVI, einer für USB (Kabelpeitsche) sowie je einer für Audio-in und -out. Zum Arbeitsplatz führen linker Hand zwei DVI, zwei USB mit aktivem Hub und ein Audioausgang für Headset oder Lautsprecher. Rechts hat G & D den Stromanschluss nebst Ein-/Ausschalter für das interne Netzteil untergebracht (siehe Abbildung).

Auf der Frontseite des Gerätes befindet sich die Tasten zum Umschalten auf dem jeweiligen Rechner mit je zwei Leuchtdioden, außerdem zwei Anschlüsse für USB – ebenfalls mit aktivem Hub –, einer für RS232 (Klinke) nebst zwei Leuchtdioden für den Arbeitsplatz. Die untere grüne Status-LED bei den Tastern zeigt an, ob der Rechner eingeschaltet ist, die obere gelbe, welcher gerade den Desktop belegt. Für den Arbeitsplatz signalisiert die grüne, dass der KVM eingeschaltet ist, während des Einrichtens blinkt die gelbe (siehe Abbildung 1).

Das Aktualisieren der Firmware erfolgt über die Servicebuchse. Auf das Adapterkabel „Klinke auf DSUB 9“ sollte man gut aufpassen, denn bei der Klinkenbuchse handelt es sich um eine

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

in der Art seltene serielle Schnittstelle. Konfigurieren kann man den KVM entweder darüber mit einem Terminalprogramm oder über die Tastatur. Der Administrator darf die Hotkeys zum Umschalten, die Zuordnung der Rechnertypen zu den Kanälen und die Art der Tastatur-Scan-Codes festlegen. Das ist nötig, weil DVIMUX außerdem Suns USB-Tastatur und -Maus sowie deren Rechner unterstützt. Für die Keyboards bietet DVIMUX die Varianten „PC Multimedia“ mit den entsprechenden Sondertasten auf der Tastatur, „PC Standard“ ohne (Nationalisierung geht über das Betriebssystem), „SUN US“ und „SUN German“ als Tastaturlayouts.

Einfach ist die Verkabelung der Videosignale, solange man es nur mit DVI zu tun hat. Bei einer Mischung von digitalen und analogen Übertragungen muss man aufpassen, hauptsächlich weil als Bildschirm nur ein TFT mit beiden Eingängen infrage kommt, die man in der Regel über eine extra zu bestellende Kabelpeitsche (DVI+VGA) zusammenfassen muss, um sie am DVIMUX anschließen zu können. Die Umschaltung zwischen analogem und digitalem Signal sollte der Monitor übernehmen.

Bei USB geht mehr als Tastatur und Maus

Im Test dienten zuerst ein Wide-22- und 15-Zoll-TFT als Monitor, anschließend löste den 22-Zöller ein gleich großer Röhrenmonitor ab. Mit der empfohlenen Kabellänge von 5 m war kein Qualitätsunterschied zwischen dem direkten Anschluss der Monitore und dem zwischengeschalteten KVM zu erkennen. Der USB-Hub erwies sich als recht umgänglich, was das Erkennen von Endgeräten betrifft, alle funktionieren, von billigen USB-Tastaturen und -Mäusen oder Adaptern für PS2 bis hin zu USB-Sticks und externen -Platten.



In Reih und Glied: Für jeden angeschlossenen Rechner gibt es fünf Anschlüsse – je zwei für DVI und Audio, einer für USB (im Bild unten). Über die Schalter kann der Anwender den Rechnern auswählen: Die obere gelbe LED zeigt, welcher gerade aktiv ist – oben im Bild (Abb. 1).

Anders sah es bei den Rechnern aus: Ein Industrie-PC auf Intel-Basis mit i855-Chipset und einem Pentium M (Sockel 479) erwies sich immer wieder als unstabil bei USB; er war nicht ohne Weiteres zur Zusammenarbeit zu bewegen. Erst ein auf der Rechnerseite zwischengeschalteter USB-Hub behob das. Der Hersteller hat zugesagt, sich darum zu kümmern.

Ein Extra gibt es, wenn mindestens ein Rechner mit zwei Grafikkarten bestückt ist, die je sowohl einen digitalen als auch einen analogen Ausgang besitzen. Hat man die passenden Kabelpeitschen angeschafft, kann man am DVIMUX8-MC2 sogar vier Monitore betreiben – zwei digitale und zwei analoge.

Fazit

Für den Fall, dass jemand bis zu acht multimediafähige Desktoprechner oder Workstations an seinem Arbeitsplatz von einer Konsole aus bedienen will und Wert auf mindestens zwei Bildschirme legt, hat Guntermann & Drunck das passende Angebot im Portfolio: DVI- und VGA- und Audio-Anschluss sowie eine Übertragungsgeschwindigkeit von 400 MHz bieten die Voraussetzungen. Zum Lieferumfang gehören die passenden DVI-Divider-Kabelpeitschen und das unbedingt notwendige spezielle serielle Update-Kabel. Wer eine höhere Bildschirmauflösung (bis 2560 × 1600 bei 60 Hz) will, muss zum DVI-MUX2 greifen, da nur dies Dual-Link unterstützt. Dabei ist der DVI-Anschluss vollständig beschaltet und die Signale gehen über zwei digitale Leitungen in einem Kabel.

Der Vorteil einer zentralen Konsole bringt den Nachteil eines beachtlichen Kabelverhaus beim DVIMUX8 mit. Pro Rechner muss der Anwender fünf Kabel verlegen, bei PS2 sind es sogar sechs. Andere Hersteller verwenden Spezialkabel, die alle bündeln. Dem steht aber bei dem Angebot von Guntermann & Drunck gegenüber, dass man die Freiheit hat, handelsübliche zu verwenden, was unter Umständen ein paar Euro einspart.

Ergonomischer wäre sicherlich ein von vorne erreichbarer Audio-Anschluss für Lautsprecher oder Headset – vor allem, wenn der DVIMUX als Gerät ins Rackgehäuse montiert werden soll.

Wer USB-Wechselmedien mit einsetzen möchte, muss hinnehmen, dass sie beim Umschalten auf einen anderen Rechner verloren gehen. Günstiger wäre ein separater Schaltweg für Wechselmedien, wie es ihn bei Blades gibt: Oben für die Konsole mit Keyboard, Video und Maus, darunter ein eigener für Speichermedien am USB-Anschluss.

Gegen den Strom schwimmend im Vergleich zu manch anderer Appliance besitzt das Netzteil über dem rückseitigen Anschluss für die Spannungsversorgung einen Ein-/Ausschalter – inzwischen eher eine Seltenheit. Eine von außen zugängliche Sicherung gibt es nicht. (rh)

Daten und Preise

DVIMUX8-MC2: 8-Kanal-KVM

Hardware: 18 DVI-Anschlüsse (zwei pro Kanal, zwei für Konsole), beschaltet analog/digital, 1920 × 1440 (75 Hz, analog), 1920 × 1200 (60 Hz, digital); vier USB 2.0 mit zwei aktiven HUBs; eine serielle Spezialkabel-Klinke auf RS232 (SubMin 9-polig); Kabelpeitsche DVI; Maße 435 × 66 × 210 mm

Hersteller: Guntermann & Drunck, www.gdsys.de

Preise: ab 1200 € (Teststellung 1841,80 €)

iX-Wertung

⊕ Übertragung analoger und digitaler Signale

⊕ handelsübliche Kabel verwendbar

⊕ klares Design

⊖ Kabelverhau

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Siggraph 2008: Neuer Hype 3D-Kino

Im Bilde

Ralf Dörner, Oliver Grau

Wer für seine Zielgruppe digitale Schläge in die Magengrube plant, war auf der Siggraph ebenso richtig wie Robotikspezialisten, denen Assistenzsysteme für die Betreuung hilfsbedürftiger Menschen vorschweben. Vorträge, Produkte und Exponate aus Forschungslaboren weltweit gaben Einblick in aktuelle Techniken der Comptergrafik und Animation.

Als Erfolg verbuchte die Special Interest Group on Graphics (Siggraph) der ACM ihre jährliche Konferenz gleichen Namens. Der mit Abstand größte internationale Event im Bereich Computergrafik und interaktive Techniken konnte in diesem Jahr knapp 28 500 Forscher, Künstler, Filmemacher und Entwickler im Bereich der grafischen Datenverarbeitung aus 87 Ländern Mitte August nach Los Angeles locken – rund 4500 mehr als im Vorjahr nach San Diego.

Passend zum breiten Spektrum der Veranstaltung, begnügten sich die Veranstalter nicht mehr mit einer einzigen Keynote, sondern haben in diesem Jahr drei Sprecher aus unterschiedlichen Branchen verpflichtet. Ed Catmull, Pioneer der Computeranimation, Mitbegründer von Pixar und nun President von Walt Disney und Pixar Animation hat das Computergrafik Labor des New York Institute of Technology gegründet und verschiedene Computergrafiktechniken maßgeblich entwickelt. Anhand der Erfahrungen, die er in herausfordernden Produktionen wie Toystory, Bug’s Life und Toystory 2 machte, versuchte er unter anderem die Frage zu beantworten, was wichtiger sei: gute Ideen oder ein gutes Team. Er ließ keinen Zweifel daran, dass Letzteres entscheidend für seinen Erfolg war.

Catherine Owens, Co-Regisseurin von „U2 3D“, der als Beispiel eines „echten“ 3D-Films in voller Länge gezeigt wurde, konzentrierte sich in ihrer Keynote auf die künstlerischen Aspekte dieses Themas. Auf technische Schwierigkeiten bei der Produktion solcher Filme gingen diverse Präsentationen aus der Filmbranche ein. „U2 3D“, der Konzertfilm der irischen Rockband, gilt in diesem Zusammenhang als Meilenstein. David Franks, Visual-Imaging-Supervisor, begründet den Erfolg des Streifens damit, dass die Stereoskopie sorgfältig eingesetzt und eventuelle Probleme in der Post-Produktion bereinigt wurden. Hürden gibt es bei der Herstellung von 3D-Filmen potenziell genug, beispielsweise zu große Disparitäten oder Kamerafehlausrichtungen, die beim Betrachter Kopfschmerzen auslösen können.

Dass die Medienwelt das Thema 3D-Stereo in den letzten Monaten stark beachtet hat, dürfte an den Animationsfilmen liegen, die in den letzten Jahren als 3D-Film ins Kino gelangten. Ermöglicht wurde dieser Trend unter anderem dadurch, dass die Spezifikation von digitalen Kinos 3D als Standard beinhaltet. Mit anderen Worten: Alle neuen nach der D-Cinema-Spezifikation ausgerüsteten Kinos können 3D-Filme abspielen. In den USA gibt es bereits viele derartiger Kinos, Europa zieht gerade nach.

Roboter analysieren Sportereignisse

Takeo Kanade, Professor für Computer Science and Robotics der amerikanischen CMU (Carnegie Mellon University) sprach in der dritten Keynote über seine 30-jährige Erfahrung im Bereich Robotik- und Computer Vision. Kanade gilt in diesem Bereich als Pionier. Insbesondere hat er im Verlauf seiner Kariere den Begriff „Virtualized Reality“ geprägt (die Konstruktion virtueller aus realen Szenen). Als einer der Ersten hat er ein Mehrkamerasystem zur Aufzeichnung menschlicher Handlungen konstruiert. Mithilfe bildbasierter Verfahren war es damit möglich, diese Handlungen aus allen Richtungen zu betrachten. Ein ähnliches System wurde später als Eye Vision zum US Superbowl eingesetzt, um Football und andere Sportarten zu analysieren. In jüngerer Zeit hat Kanade sich dem Thema „Science of Everyday Living“ verschrieben. Dabei erforscht er,

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

wie Computer Vision im täglichen Leben Einsatz finden kann. Erlaubt man dem Computer beispielsweise, die Sicht einer Person im Alltag einzunehmen und zu verstehen, was sie gerade tut, könnten daraus, gepaart mit Robotik, für Menschen im hohen Alter akzeptable Assistenzsysteme entstehen.

Roboter waren auch ein Thema im Rahmen der „New Tech Demo“ (früher: Emerging Technologies). Der Prototyp des MDS (Mobile-Dexterous-Social) Robot for Human-Robot Teamwork ist das Ergebnis einer Kollaboration zwischen MIT, University of Massachusetts Amherst, Xitome Desing + Meka Robotics LLC. Die Augen des Roboters sind mit jeweils einer Kamera bestückt, dazu kommt eine weitere in der Stirn des Roboters. Das System erkennt Gesichter und verfolgt diese. Dabei schauen einen die Augen an – ein sehr irritierendes Gefühl.

Einen kleinen Schritt in Richtung Holodeck gehen die Shinoda Labs, die durch Interferenzen von Ultraschall haptisches Feedback quasi aus dem Nichts erzeugen: Man bewegt seine Hand durch die Luft und spürt an bestimmten Stellen plötzlich Druck und kann zum Beispiel eine virtuelle Fläche erfühlen. Kräfte lassen sich an Punkten mit circa 1 cm Durchmesser erzeugen, die in einem Gitter angeordnet kombiniert werden können – allerdings ist die Wirkung noch recht schwach und diffus.

Wesentlich stärkere Kräfte bei höherer Feinfühligkeit erzeugt ein Gerät von Butterfly Haptics, das darauf basiert, dass ein Griff in einem Magnetfeld in der Schwebe gehalten wird. Dies umgeht Nachteile mechanischer Haptik-Geräte wie Reibung oder Motorprobleme. Allerdings ist das Gerät mit über 30 000 € nicht gerade billig.

Haptisches Feedback von Boxhieben in die Magengrube lässt sich ebenfalls vermitteln. Dazu passt die 3DVs ZCam, die als Sensor für Tiefeninformationen dient und beispielsweise die Entfernung der Hände vom Bildschirm ermitteln kann. Damit lässt sich, wie auf der Siggraph gezeigt, ein Boxspiel realisieren, bei dem der Spieler einfach die Fäuste ballt und loslegt – ohne ein Eingabegerät zu halten. Das Ganze soll in einem Jahr zum verbraucherfreundlichen Preis von 100 $ auf den Markt kommen.

Einen derartigen Tiefensensor nutzt auch der IncreTable, unter anderem entwickelt von der FH Hagenberg. Der Tisch realisiert multimodale Interaktion: Auf der Tischplatte werden reale Gegenstände angeordnet, die ein Sensor erfasst. Anhand dieser Information erzeugt der Computer ein passendes Bild und projiziert es auf den Tisch. So kann man etwa eine reale Rampe auf dem Tisch platzieren über die ein virtuelles Auto fliegt. Ähnliche Aufbauten sind unter anderem die schon als Produkt erhältliche Tangible Workbench von Kommerz oder UlteriorScape von der Universität Tokio, bei der die Tischplatte aus einem speziellen Material gefertigt ist, das ein Einspeisen des Bildes von der Seite erlaubt. Gleichzeitig ist das Material lichtdurchlässig von unten, sodass ein zweites Bild projiziert werden kann, das zum Beispiel erst dann auf einem Stück Papier sichtbar wird, wenn jemand es über die Tischplatte hält.

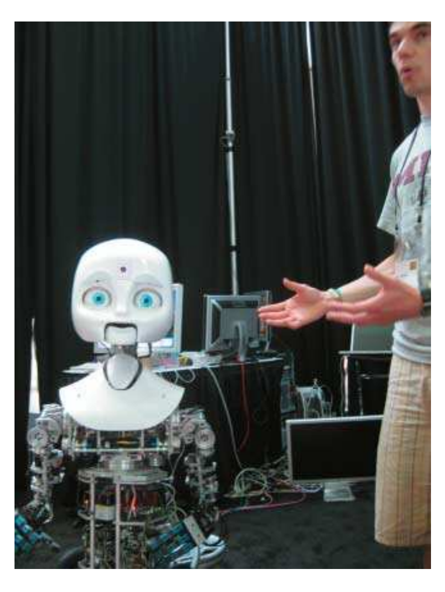
Ein Blick in die Kristallkugel

Zu den New-Tech-Demos zählten auch wieder AR-Systeme (Augmented Reality) wie AR Scope der Universität Tokio. In diesem Projekt hält der Benutzer eine Art Kristallkugel in den Händen, die er vor ein reales Objekt – etwa einen Apfel – halten kann. Durch die Kristallkugel sieht er nach wie vor das Bild der Realität, dieses lässt sich aber durch computergenerierte Anteile ergänzen. So kann ein virtueller Wurm am Apfel nagen oder der Apfel plötzlich blau erscheinen. Das System arbeitet mit einer retro-reflektiven Projektionstechnik und erlaubt beliebige Blickpunkte. Anders als bei der Verwendung herkömmlicher Displays wird das augmentierte Bild ohne Rahmen in die Realität eingeblendet.

Eine interessante Variante der in der AR häufig eingesetzten Marker (erleichtern dem Computer das maschinelle Auswerten des Live-Videobildes) haben japanische Forscher aus Tokio gleich in mehreren Exponaten demonstriert: Das Marker-Muster wird auf verformbares Material aufgebracht, und das Berühren oder Drücken führt dann zur Änderung des Musters. Eine Kamera erkennt diese Modifikation und wertet sie aus.

Wie man es vom Standort Los Angeles gewohnt ist, war die begleitende industrielle Ausstellung gut besucht. Die Anzahl von 246 Ausstellern ist auf gleichem Niveau verglichen mit den 236 vom letzten Jahr in San Diego.

Natürlich gab es auch hier einiges zum Thema 3D-Stereo. So demonstrierten beispielsweise am Stand des 3D Consortium (siehe auch S. 25) verschiedene Hersteller ihre 3D-Displays.



Die schönen Augen des Mobile-Dexterous-Social Robot irritieren den Anwender durch direkten Augenkontakt (Abb. 1).

Die Displaytechnik gilt als Schlüssel für einen Erfolg von 3D-Stereo im Privatbereich. Zu den Displays, die in verschiedenen Inkarnationen in den letzten 10 Jahren auf Ausstellungen wie der Siggraph zu bewundern waren, sind nun einige preislich erschwingliche Geräte hinzugekommen, die nach dem Polarisationsprinzip arbeiten. Der Betrachter benötigt hierbei eine Brille mit Polarisationsgläsern. Eine beeindruckende Palette von LCD-Geräten mit drei verschiedenen Auflösungen und zusätzlich einem autostereoskopischen Display bietet die koreanische Firma Miracube an. Die Preisspanne wurde (vorbehaltlich) mit 2000 US-$ (19 Zoll, 1280 × 640 × 1024 Auflösung) bis hin zu 5000 US-$ angegeben.

Motiontracking auch für wenig Geld

Eine beeindruckende Vielfalt an Systemen haben Hersteller zum Thema Motion-Capture ausgestellt. Vertreten waren hier die Markführer Vicon und Motion Analysis mit ihren bekannten markerbasierten, optischen Systemen. Neu waren Produkte, die entweder keine Marker benötigen, wie das optische System der Firma Organic Motion oder das von Xsens Technologies B.V., das mit Trägheitssensoren arbeitet. Ferner waren Firmen vertreten, die ihre Chancen im Niedrigpreissegment suchen: OptiTrack bietet ihr optisches Mehrkamerasystem zum Preis von 5000 US-$ an. Die russische Softwarefirma iPi Soft will gegen Ende des Jahres gar eine Software herausbringen, die entweder mit einer oder zwei Webkameras arbeitet und zum

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Preis von 250 US-$ (eine Kamera) beziehungsweise 950 US-$ (zwei Kameras) zu haben sein soll. Die gezeigten Demos versprechen keine professionelle Qualität, mögen aber für die eine oder andere semiprofessionelle Webanwendung genügen.

Berührungsloses Tracking ist nach wie vor ein Forschungsthema, ein Technical Paper beschäftigte sich etwa mit dem berührungslosen Tracking von Kleidung. Tobii stellte ein in einem Monitor integriertes berührungsloses Tracking-System vor, dass die Blickrichtung des Benutzers ermittelt. So kann man allein durch das Anschauen eines Schachfeldes auf dem Bildschirm eine Figur dorthin bewegen. Das ab 10 000 € erhältliche System ermöglicht unter anderem die Interaktion von Querschnittsgelähmten mit dem Computer.

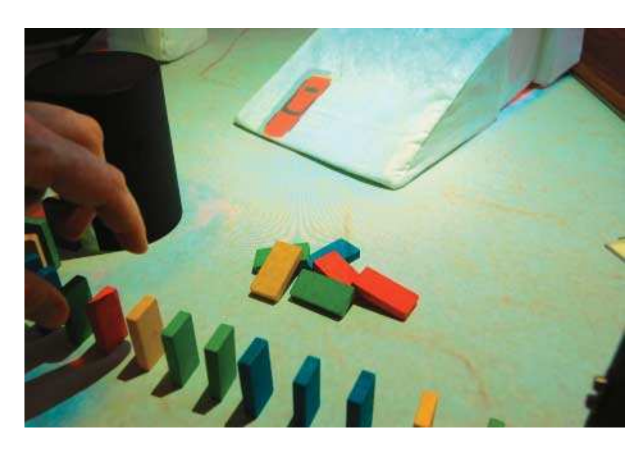
Grafikhardware für Profianwendungen

Auf dem Stand von Nvidia waren insbesondere Lösungen und Anwendungen aus dem professionellen Bereich zu finden. Eindrucksvoll demonstrierte der Hersteller die Leistungsfähigkeit des neuen Quadro Plex 2200 D2: Eine von Nvidia programmierte Software zeigte volles Raytracing eines 2-Millionen-Vertex-Modells mit einer Trace-Tiefe von bis zu 5 bei einer maximalen Bildwiederholrate von 30 fps. Die Systeme der Plex-Reihe sind in zwei Formkonfigurationen zu haben: Die Deskside-Systeme sehen aus wie ein Desktop-Computer und werden neben einer Workstation aufgestellt. Die zweite Variante lässt sich in ein Rack einbauen.

Außerdem zu sehen waren Produkte der Tessla-Serie. Dies sind Komponenten, die zwar einen zentralen Grafikprozessor (GPU) haben, aber keinen Grafikausgang besitzen. Ihr Einsatzgebiet liegt in Datenverarbeitungsanwendungen, die beispielsweise mit Nvidias CUDA (Compute Unified Device Architecture) programmiert wurden.

Ein viel diskutiertes Thema war Larrabee, Intels neue Architektur mit multiplen x86 CPU Cores, die die Marktdominanz der GPUs von ATI und Nvidia anfechten soll. Bei den Cores handelt es sich um In-Order Pentium 1 CPUs, die auf 64 Bit aufgerüstet und mit einer Vector-Unit versehen wurden. Der Datenaustausch zwischen den Cores erfolgt über den globalen L2 Cache, der in lokale Teilmengen der Größe 256 KByte pro Core gegliedert ist. Der so entstehende Parallelrechner lässt sich wie gewohnt in C oder C++ programmieren, wie gewohnt erfolgt auch das Debugging des Codes. Intel hat auch gleich gezeigt, wie man mit Larrabee Bilder erzeugen kann, und einen zur Hardwarearchitektur passenden Rendering-Algorithmus vorgestellt, der auf Binning basiert (das heißt, die darzustellenden Dreiecke werden in Bins aufgeteilt, die einem bestimmten Bildteil zugeordnet sind), um unter anderem die benötigte Speicherbandbreite zu reduzieren.

Im Gegensatz zur GPU sind fast alle Schritte der Renderpipeline in Software realisiert – bis auf die Texture Unit, die im selben virtuellen Speicherbereich wie die Cores angesiedelt ist, gibt es keine Fixed Functionality. Das bedeutet, mehr Flexibilität, zum Beispiel lässt sich die Rasterisierung – ein Schritt der Renderpipeline, der bei GPUs in Hardware fixiert ist – bei Larrabee in Software programmieren. Gleiches gilt für die Verarbeitung der Fragmente am Ende der Renderpipeline. So lassen sich Effekte mit Transparenz und Nebel erreichen, die bei heutigen GPUs nicht möglich sind. Sogar das Scheduling, also die Verteilung der Daten auf die einzelnen Recheneinheiten, lässt sich in Larrabee durch Software flexibel gestalten. Bei den GPUs geschieht dies nach einem nicht änderbaren Algorithmus. Nicht zuletzt ist man in den Datenstrukuren etwa von Framebuffer und Stencil-Buffer nicht mehr auf 2D-Arrays festgelegt und könnte etwa verkettete Listen einsetzen.



Ein auf dem IncreTable von einem Sensor erfasstes Spielzeugauto fliegt als virtuelles Abbild über eine reale Rampe (Abb. 2).

Schneller durch Parallelität

Intel verspricht sich von Larrabee nicht nur die effiziente Verarbeitung von Daten mit hoher Parallelität, sondern auch die parallele Abarbeitung unterschiedlicher Aufgaben gepaart mit der Möglichkeit, nahtlos sequenziellen Code auszuführen. Auch Sony stellte seine neue Multi-Core-Plattform ZEGO („Zest to Go“) vor, bei der der Cell-Broadband-Engine-Mikroprozessor eingesetzt wird. Das erste ZEGO-Produkt für HD-Videoproduktion, BCU-100, soll noch in diesem Jahr auf den Markt kommen.

Parallelverarbeitung kristallisiert sich als der wesentliche Weg für künftige Performanzsteigerungen heraus: „Computer get wider not faster.“ Computergrafik ist hier ein von einem großen Consumer-Markt getragener Vorreiter. Die dort geleisteten Entwicklungen übertragen die Hersteller immer mehr auf andere Gebiete der Informatik. Schließlich profitieren auch Nicht-Grafikanwendungen wie Text Indexing von einer Parallelrechenleistung, die bei den GPUs die Teraflop-Marke überschreitet. Damit werden auf der Siggraph vorgestellte Techniken für IT im Allgemeinen immer interessanter.

Ähnlich wie Nvidia mit CUDA trägt Microsoft mit dem in DirectX 11 neu eingeführten Compute Shader dieser Entwicklung Rechnung. Der Compute Shader unterstützt unter anderem Random Access I/O und Data Sharing zwischen GPU-Threads. In eine ähnliche Richtung geht die Open Computing Language (OpenCL). Basierend auf einem Vorschlag von Apple soll OpenCL ein neuer Standard für Heterogeneous Computing zwischen CPU und GPU werden – insbesondere für Anwendungen außerhalb der Grafik. OpenCL wird mit OpenGL abgestimmt werden, um einen effizienten Datenaustausch zu gewährleisten (zu OpenGL 3.0 siehe S. 106).

Die größere Flexibilität bei der Hardwareunterstützung lässt andere Verfahren der Bilderzeugung neben der Rasterisierung wie Voxel Rendering oder Raytracing immer interessanter werden. Zwar gab es auf der Siggraph

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Demonstrationen von Raytracing in Echtzeit – zum Beispiel von Nvidia oder IBM –, aber für eine wirklich herausragende Bildqualität müsste die Anzahl der Rays um mindestens eine Größenordnung erhöht werden. Doch selbst eine Verkürzung der für das Rendering anfallenden Zeiten beim Raytracing bringt schon eine spürbare Verbesserung: Die aktuellen Wartezeiten auf Bilder sind ein großes Produktionsproblem, das die iterative Arbeitsweise der Künstler hemmt. Eine Beschleunigung könnte hier nicht nur die visuelle Qualität, sondern nach Ansicht von Experte Jon Peddie unter anderem auch das Spielerlebnis bei Computerspielen verbessern. Interessant sind die auf der Siggraph diskutierten hybriden Ansätze. So hilft eine Shadow Map aus der Rasterisierung das Raytracing zu beschleunigen.

Die Evolution schreitet weiter voran

Passend gewählt war das diesjährige Motto „Evolve“ für die 114 technischen Vorträge, da die wissenschaftlichen Beiträge nichts revolutionär Neues boten. Viele Papers stellten Verbesserungen und Erweiterungen früherer Beiträge vor. So präsentierten Wissenschaftler einen Ausbau ihres Systems zur automatischen Größenanpassung von beliebigen Bildern, das letztes Jahr einige Aufmerksamkeit erlangte. Der als Seam-Carving bezeichnete Ansatz nimmt automatisch redundante Bereiche eines Bildes heraus oder kann sie umgekehrt wieder einfügen, sodass sich das Bild in Grenzen beliebig horizontal oder vertikal verkleinern oder vergrößern lässt, ohne den Bildinhalt merklich zu verändern. Ein denkbares Anwendungsbeispiel wäre die Anpassung eines Bildes in einer Webseite. Dieses Jahr präsentierten die Autoren die Erweiterung auf Videos, die noch nicht perfekt arbeitet, jedoch ebenfalls interessante Anwendungen verspricht.



Durch Facetracking können digitale Figuren ihren Gesichtsausdruck schnell einer neuen Stimmung anpassen (Abb. 3).

In derselben Session war eine Verfeinerung des „Photosynth“-Systems zu sehen, das Microsoft bereits 2006 auf der Siggraph vorgestellt hat. Die Software analysiert automatisch Fotosammlungen (wie Flickr) und extrahiert die 3D-Struktur eines Gebiets sowie die Position der Kamera während der Aufnahme der Bilder. Dieses Jahr wurde ein Ansatz dargelegt, der automatisch einen Pfad zwischen Bildern berechnet, die an einem Standort aufgenommen wurden. Der Benutzer kann dann quasi in 3D von einem Bild zum nächsten navigieren.

Eine innovative Anwendung zum Thema Videobearbeitung hatte der europäische Zweig der Microsoft-Forschung parat: Mithilfe einer Repräsentation, die auf einer dreidimensionalen Darstellung eines Objekts basiert, wird es möglich, dieses in einem Video zu manipulieren. Dabei entsteht eine Art Mosaik des Objekts, das alle Ansichten in einem Bild vereint, das der Anwender manipulieren kann. Die Änderungen projiziert die Software zurück in das Video, wo sie dem bewegten Objekt „anhaften“.

Israelische Forscher haben ein Verfahren vorgestellt, wie man die visuelle Qualität von Fotos im wahrsten Sinne des Wortes erhöhen kann – indem man die darauf abgebildeten Gesichter attraktiver macht. Tatsächlich können subtile Veränderungen beispielsweise von Proportionen Menschen auf Fotos schöner aussehen lassen. Der Algorithmus erkennt 48 Landmarken in einem Gesicht, die zum Teil manuell nacheditiert werden müssen. Danach geht alles automatisch: Der Computer verändert das Bild des Gesichts systematisch und bewertet das Ergebnis – dank maschinellem Lernen lässt sich ein Score ermitteln, wie attraktiv ein Gesicht wirkt. Das Ergebnis mit dem höchsten Score wird dann präsentiert. Dabei kann der Anwender wählen, ob das Gesicht nun für Männer oder Frauen attraktiver wirkt und mittels Schieberegler einstellen, was wichtiger ist: Attraktivität oder Ähnlichkeit zum ursprünglichen Foto. Sollte das Ergebnis nicht zufriedenstellend sein, kennen Forscher der Columbia University eine drastische Lösung. Ihr Verfahren ermöglicht es, Gesichter auf Fotos komplett auszutauschen. Anwendungen bestehen zum Beispiel darin, Menschen in Systemen wie Google Street View aus Datenschutzgründen unkenntlich zu machen, ohne dass die Gesichter verschwommen erscheinen müssen.

Von dem angekündigten organisatorischen Umkrempeln der Siggraph war wenig zu spüren – mal sehen wie es im nächsten Jahr in New Orleans wird (3. bis 7. August). Davor richten die Organisatoren die erste Siggraph Asia vom 10. bis 13. Dezember in Singapur aus, um der zunehmenden Bedeutung des asiatischen Raumes Rechnung zu tragen. (ka)

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Bund plant Grundlagen für sichere Kommunikation

Schutzbefohlen

Christoph Wegener, Dennis Werner

Die Bundesregierung plant im Rahmen von „E-Government 2.0“ neben dem elektronischen Personalausweis technische und rechtliche Rahmenbedingungen für eine „sichere und verbindliche elektronische Kommunikation“. Grundpfeiler dieser Bemühungen sollen die sogenannten Bürgerportale mit den De-Mail-Diensten sein.

Allen bisherigen technischen und rechtlichen Bemühungen zum Trotz sinkt das Vertrauen der Bürger in die Sicherheit der Internet-Kommunikation – kein Wunder angesichts Malware, Spam und Angriffen per „Social Engineering“. Ohne weitere Vorkehrungen weisen sowohl die klassische E-Mail als auch die weit verbreiteten Authentifizierungsmechanismen an Internetportalen teilweise eklatante Sicherheitsmängel auf. Bürger, E-Commerce-Anbieter und Behörden können sich bei der Kommunikation per E-Mail daher nicht darauf verlassen, dass vertrauliche Informationen geschützt und E-Mails unverändert bleiben oder dass sie überhaupt den gewünschten Adressaten erreichen. Entsprechend bleibt der elektronischen Kommunikation in weiten Teilen auch die Anerkennung durch unsere Rechtsordnung – zumindest auf Beweisebene im Prozess – verwehrt.

Eine Ausnahme bilden die praktisch wenig erfolgreichen E-Mail-Verfahren, die eine qualifizierte elektronische Signatur nach dem Signaturgesetz erfordern. Es bleibt dabei, dass Vertragspartner, die Geschäfte im Internet abschließen, dies weitgehend auf eigene Gefahr tun und im Falle eines Prozesses meist ohne verwertbare Beweismittel dastehen. Solche Unsicherheiten belasten zurzeit vor allem die E-Commerce-Anbieter. An umfangreiche E-Government-Anwendungen ist in einer solchen Umgebung erst recht nicht zu denken, und entsprechend haben sich bislang nur Angebote in Randbereichen des E-Government entwickelt.

E-Government kryptografisch gesichert

Dieser Entwicklung möchte die Bundesregierung nun entgegenwirken. Ausgehend vom Aktionsplan „E-Government der europäischen Initiative i2010“, den Erfahrungen mit „BundOnline 2005“ und „Deutschland-Online“ hat die Bundesregierung bereits im Jahre 2006 das Programm „E-Government 2.0“ als Konkretisierung eines Teils der Gesamtstrategie im Regierungsprogramm „Zukunftsorientierte Verwaltung durch Innovation“ beschlossen. Die Umsetzung des Programms erfolgt durch alle Bundesressorts hinweg, die Koordinierung liegt beim Bundesministerium des Innern.

Die Basis eines sicheren Kommunikationsraums im Internet sollen Bürgerportale und der De-Mail-Dienst bilden. Beides soll eine sichere und rechtlich verbindliche Authentifizierung und elektronische Kommunikation für E-Commerce- und E-Government-Szenarien sicherstellen und erfordert ein abgestimmtes Konzept technischer Maßnahmen und rechtlicher Rahmenbedingungen. Das Konzept für Bürgerportale und die Planungen zur Einführung eines elektronischen Personalausweises (ePA) in der Arbeitsgruppe 4 „Sicherheit und Vertrauen in IT und Internet“ hat die Bundesregierung im Rahmen des zweiten Nationalen IT-Gipfels im Dezember 2007 vorgestellt. Im Konzept der Bürgerportale bildet die Einrichtung einer E-Mail-Alternative unter der Bezeichnung „De-Mail“ (früher „D-Mail“, aber wegen markenrechtlicher Bedenken geändert) einen der Schwerpunkte.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Daneben soll ein „Dokumentensafe“ der langfristigen, sicheren elektronischen Archivierung dienen. Der ePA als hoheitliches Dokument soll etwa für Kontoeröffnungen, Adressverifikationen und Altersnachweise einsetzbar und darüber hinaus optional mit einer qualifizierten elektronischen Signatur versehen sein. Er wird zudem biometrische Merkmale – etwa ein biometrietaugliches Lichtbild – enthalten, Fingerabdrücke aber, zumindest nach aktueller Planung, nur auf freiwilliger Basis.

Erst E-, dann De-Mail

Nach den Vorstellungen der Bundesregierung folgt der Aufbau eines sicheren Kommunikationsraums im Internet einem Geschäftsmodell, in dem privatwirtschaftliche Dienstleister – die sogenannten Bürgerportaldiensteanbieter (BPDA) – die Infrastruktur aufbauen und im Rahmen eines von einer Bundesbehörde durchgeführten Zertifizierungsverfahrens nachweisen sollen, dass sie ein hohes Niveau an Datensicherheit sowie Daten- und Verbraucherschutz

Firmen benötigen andere Adressen als Privatleute. Wer nicht durch seine Mailadresse identifizierbar sein möchte, kann sich ein De-Mail-Pseudonym zulegen (Abb. 1).

	Typ	De-Mail-Adresse
1.	Privatperson	[vorname.nachname.#@]BPDA.zertIT.de Beispiel: Markus.Meier.2@BPDA.zertIT.de
2.	Pseudonym	[ps_pseudonym@]BPDA.zertIT.de Beispiel: ps_Mickey.Mouse@BPDA.zertIT.de
3.	Firma	[abteilung@firma].BPDA.zertIT.de Beispiel: Einkauf@Photo-Meier.BPDA.zertIT.de

iX-TRACT

- Dem heutigen E-Mail-Standard mangelt es an Vertraulichkeit, Integrität sowie an der Beweisbarkeit von Sende- und Empfangsvorgängen.
- Für die rechtssichere digitale Kommunikation zwischen Bürgern, Behörden und Unternehmen sieht die Bundesregierung die De-Mail-Infrastruktur vor, die auf gewohnten Internetdiensten wie E-Mail und Web basiert.
- De-Mail-Anwendern stehen drei Sicherheitsstufen für die Kommunikation sowie ein Datentresor zum Ablegen privater, sensibler Daten zur Verfügung.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

bieten. Auf dieser Grundlage soll ein Verbund zertifizierter Bürgerportale entstehen, der sich entweder durch Einsparungen in Wirtschaft und Verwaltung (etwa durch Wegfall des Rechnungsversandes) oder durch ein „E-Porto“ finanzieren soll.

Im Vordergrund der technischen Umsetzung steht, den Bürgern einen Zugriff mit gewohnten Verfahren und verbreiteter Software zu ermöglichen, also per Webbrowser und E-Mail-Client. Die Bürgerportale sollen möglichst ohne dedizierte Client-Software und ohne zusätzliche Hardware nutzbar sein. Grundlage für De-Mail wird daher die herkömmliche E-Mail sein: Auf Basis von Standardformaten und -protokollen sollen Erweiterungen entstehen, die Sicherheit und Vertraulichkeit gewährleisten. In besonders kritischen Bereichen dient die Einbindung des elektronischen Personalausweises der Authentifizierung.

De-Mail-Accounts sollen sowohl natürlichen als auch juristischen Personen zur Verfügung stehen. Die Registrierung erfordert nach aktueller Planung eine zuverlässige Identifizierung, etwa mittels Post-Ident. Eine standardisierte Struktur auf Basis einer eigenen Second-Level-Domain (möglicherweise zertIT.de) soll für die Kommunikationspartner erkennbar machen, dass es sich um eine geprüfte und authentische Adresse handelt.

Verifizierte Adressen kostenlos

Für Adressen natürlicher Personen ist das Format „vorname(n).nachname [.nummer]@BPDA.zertIT.de“ vorgesehen, zum Beispiel „Markus.Meier. 2@BPDA.zertIT.de“. Neben diesen Adressen, die den Namen des Inhabers enthalten, sollen auch pseudonyme Adressen erhältlich sein, die einen gesonderten Zusatz „ps_“ in der Adresse (etwa „ps_Mickey.Mouse“) tragen. Adressen juristischer Personen sollen dagegen wie folgt aussehen: „local-part@[subdomain.]name.BPDA.zertIT. de“. Dabei ist „subdomain“ quasi der Name der Institution, also so etwas wie „Photo-Meier“ und „local-part“ die dortige Abteilung oder Person, also zum Beispiel „Einkauf“. Ein vollständiges Beispiel könnte wie folgt lauten: „Einkauf@Photo-Meier.BPDA.zertIT.de“.

So gut strukturierte Adressen haben allerdings nicht nur Vorteile. Jeder Bürger, also auch jeder Spammer, kann sich schnell zusammenreimen, wer welche De-Mail-Adresse hat. Im Zweifel genügt es, Daten aus Telefonverzeichnissen (eventuell mit Nummernerweiterung und bei allen BPDAs) zu testen. Die Einführung eines Pseudonyms nützt nichts, da es ja nur zu einer zusätzlichen Adresse führt und die Hauptadresse weiterhin gilt. Lediglich ein Flag, ob man den Empfang und Versand von De-Mails aus dem und ins Internet erlauben will, soll einen gewissen Schutz bieten. Das wirft aber die Frage auf, ob Nutzer ihren De-Mail-Account überhaupt entsprechend einschränken werden.

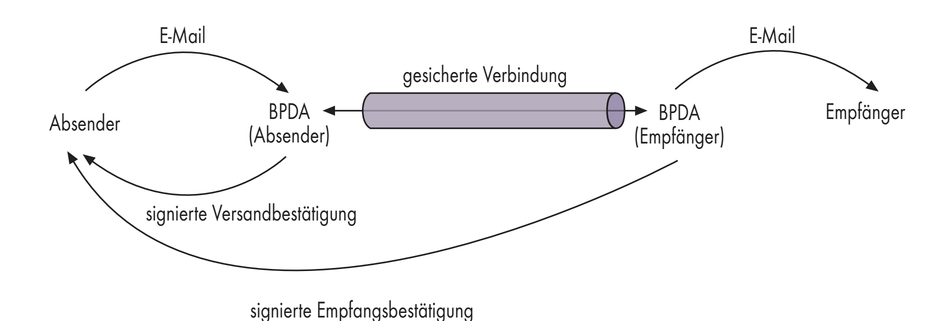
Erschwerend kommt hinzu, dass nach aktueller Planung (Stand: August 2008) innerhalb des BPDA-Netzwerks keine strikte Spam-Filterung, sondern nur ein „Taggen“ vermeintlicher Spam-Nachrichten stattfinden soll. Man argumentiert, dass nur registrierte Nutzer Zugang zu De-Mail bekommen können und Spam deswegen keine Rolle spiele. Malware-verseuchte PCs, die als Spam-Schleudern über reguläre, aber gekaperte Accounts arbeiten können, spielen wohl noch keine Rolle bei den Überlegungen. Etwaigen Schutz bietet eventuell die Tatsache, dass der Nutzer beim Authentifizierungsniveau „normal“ (dazu später mehr) nur eine begrenzte Anzahl von De-Mails pro Zeiteinheit verschicken können soll. Auch die Eintragung von De-Mail-Adressen in amtliche Melderegister birgt Zündstoff. Ob dies auf freiwilliger Basis oder zwangsweise erfolgen wird, steht noch nicht fest.

Für De-Mail-Accounts sind drei Authentifizierungsstufen geplant. Das Niveau „normal“ verlangt lediglich Benutzernamen und Passwort und geht damit nicht über den heute üblichen Sicherheitsstandard hinaus. Entsprechend sind Nachrichten auf diesem Sicherheitsniveau nicht rechtsverbindlicher als heutige E-Mails. Das Sicherheitsniveau „hoch“ erfordert eine Authentifizierung durch ein auf Besitz und Wissen basierendes Verfahren. Nur das Niveau „sehr hoch“ erfordert den Einsatz spezieller Authentifizierungsfunktionen hoheitlicher Identitätsdokumente, etwa die eID-Funktion des ePA. Ab dem Sicherheitsniveau „hoch“ kann De-Mail dazu beitragen, den Schutz vor Identitätsdiebstahl im Internet zu verbessern.

Elektronische Einschreiben

Außerdem soll De-Mail verschiedene Versandarten bereitstellen. Die einfache De-Mail gleicht dabei der heutigen E-Mail. Das De-Mail-Einschreiben hingegen liefert darüber hinaus einen rechtssicheren Zustellnachweis. Das kann insbesondere bei fristgebundenen Willenserklärungen von erheblicher Bedeutung sein. Zunächst stellt der Absender-BPDA eine Versandbestätigung aus. Der Empfänger-BPDA liefert eine Eingangsbestätigung, sobald die De-Mail im Postfach des Empfängers ankommt – unabhängig davon, ob dieser die betreffende De-Mail überhaupt zur Kenntnis nehmen konnte. Für die Einhaltung rechtlicher Fristen kann das äußerst wichtig sein (dazu später mehr). Neben den genannten kommunikativen Funktionen sollen die Bürgerportale zukünftig mit dem sogenannten Ident-Verfahren eine weitere Komponente enthalten, die dem Nachweis einzelner Identitätsmerkmale dienen soll.

De-Mail protokolliert nicht nur den Sende- und Zustellzeitpunkt, sondern mittels Hash-Wert auch den Inhalt einer Nachricht – zumindest denjenigen, den die BPDA weiterleiten. Dieser muss nicht mit dem Inhalt übereinstimmen, den der Absender schreibt oder den der Empfänger liest: Eine Malware könnte die Daten verfälscht haben. Wenn Absender und Empfän-



De-Mail sieht neben kryptografisch gesicherten Kommunikationskanälen auch das Signieren der Mail-Inhalte durch die Bürgerportaldiensteanbieter (BPDA) vor (Abb. 2).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ger die in der Bestätigung enthaltenen Hash-Werte nicht nochmals mit der versandten Nachricht vergleichen, wiegen sie sich damit in trügerischer Sicherheit. Wie dem Hauptadressaten der Initiative, Otto Normalbürger, die Verifikation der Hash-Werte sicher gelingen soll, bleibt bisher unbeantwortet – ebenso die Frage, wie er etwa im Falle eines Prozesses belegen soll, dass er den (per Hash-Wert bestätigten Inhalt) nicht selbst verfasst hat.

Safe für Dokumente

Zurzeit gibt es für Otto Normalbürger keinen einfachen und praktikablen Weg, Dokumente rechtssicher elektronisch zu archivieren. Im Rahmen der Bürgerportale einzurichtende Dokumentensafes sollen diese Lücke schließen – und bei Bedarf einzelne Dokumente Dritten – vom Besitzer konfigurierbar – „zur Ansicht“ oder „zum Download“ zur Verfügung stellen.

Technische Details des Dokumententresors sind noch nicht spezifiziert. Allerdings steht bereits die interessante Tatsache fest, dass eine Dateiverschlüsselung lediglich als optionales Feature in der Hand des Nutzers liegen soll. Ob der BPDA die Dokumente im Safe wenigstens zum Schutz vor unliebsamen Mitlesern standardmäßig verschlüsseln soll (womit er natürlich einen Nachschlüssel hätte), ist derzeit nicht Gegenstand der Diskussion. Die Authentifizierung soll per Anmeldung mit dem ePA erfolgen. Um einen nachhaltigen Nutzen für den Bürger zu erzielen und um die breite Masse vom Nutzen zu überzeugen, sind vor allem Usability- und Sicherheitsprobleme zu lösen.

Wo bleibt der Datenschutz?

Einen Speicherplatz im öffentlich zugänglichen Internet anzubieten, der persönliche, sensible Dokumente enthält, ähnelt nicht zuletzt dem Abstellen eines Banktresors auf offener Straße. Eine solch zentrale und zugleich gut zugängliche Dokumentensammelstelle dürfte Internetkriminellen ein lohnendes Ziel bieten. Derzeit erscheint es wenig Erfolg versprechend, sicherheitsbewussten Bürgern das geschilderte Konzept schmackhaft zu machen.

Zentrale Rechtsfragen stellen sich insbesondere rund um den Schutz der im Rahmen der eID-Funktion gespeicherten Daten. Er besteht darin, dass der Zugriff nur nach Eingabe einer geheimen PIN möglich ist und der Inhaber auf diese Weise die Kontrolle über die Datenfreigabe behält. Das Auslesen der Daten erfolgt zudem über einen verschlüsselten Kanal zwischen dem Chip und dem beteiligten Diensteanbieter – etwa einem Onlinehändler. Das soll verhindern, dass eine lokale Software mitliest.

Zugreifen dürfen generell nur zertifizierte Diensteanbieter, deren Zertifikate der Chip überprüft. Ob die Ablehnung anderer Anbieter wettbewerbsrechtlich überhaupt Bestand haben kann, bietet Stoff für rechtliche Diskussionen. Auf diese Weise kann aber eine gegenseitige Authentifizierung erfolgen. Das ist generell zu begrüßen, denn es erschwert Angriffe – etwa durch Phishing – erheblich.

Die Mindestanforderungen an das Sicherheitsniveau von Bürgerportalen

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ergeben sich nicht zuletzt aus rechtlichen Überlegungen, die in die Gestaltung der Technik einfließen. Auf der anderen Seite müssen sich die rechtlichen Rahmenbedingungen laufend an die technische Entwicklung anpassen.

Recht und Technik beeinflussen einander

Die rechtliche Seite verfolgt vor allem das Ziel, elektronische Kommunikation auf eine Stufe mit herkömmlichen, papierbasierten Verfahren zu stellen. Dies soll zu mehr Rechtssicherheit für Verbraucher, Unternehmen und Behörden führen. Beim Umgang mit E-Mail- und anderen Accounts im elektronischen Geschäftsverkehr stellen sich bisher vor allem die Fragen nach dem Zugang von Willenserklärungen und deren Nachweis – und danach, wie sich der Missbrauch von Accounts ausschließen lässt.

Willenserklärungen, auch elektronisch abgegebene, werden grundsätzlich mit dem Zugang beim Empfänger wirksam. Das betrifft Vertragsangebote und -annahmen ebenso wie die Ausübung von Rücktritts- oder Widerrufsrechten. „Zugang“ bedeutet, dass die Erklärung derart in den Machtbereich des Empfängers gelangt, dass er Kenntnis davon nehmen kann. In der realen Welt gilt das etwa dann, sobald ein Brief in den Briefkasten des Empfängers fällt. E-Mails sind nach herrschender Meinung unter Juristen zugegangen, sobald sie der E-Mail-Server des Empfängers speichert.

Schuldfrage eindeutig geklärt

Das Übermittlungsrisiko trägt, bis auf den Ausnahmefall einer bewussten Zugangsvereitelung, grundsätzlich der Absender einer Nachricht. Im Rahmen eines Rechtsstreits muss der jeweilige Absender beweisen, dass seine Willenserklärung tatsächlich zugegangen ist. Im Fall einfacher Briefe und E-Mails kann er das in der Regel nicht. In der realen Welt bedient man sich daher für Willenserklärungen, deren Zugang wichtige Rechtsfolgen hat (etwa Kündigungen), entweder eines persönlichen Boten, der als unabhängiger Zeuge zur Verfügung steht, oder eines Einschreibens mit Rückschein. Beides bietet die aktuelle E-Mail-Infrastruktur nicht. Entsprechend gelingt der Zugangsnachweis einer E-Mail selten. De-Mail soll nun Rechtssicherheit schaffen, da sich die Zustellung – je nach Versandart – sicher nachweisen lässt.

Allerdings gilt dies nur für die Einlieferung in die Mailbox des Empfängers. Ob derjenige den Inhalt vielleicht gar nicht zur Kenntnis nehmen konnte – etwa wegen eines Ausfalls seiner Internetanbindung oder eines Hardwareschadens beim empfangenden BPDA – spielt keine Rolle. Das ist – vielen Kritikern zum Trotz – kein Novum der elektronischen Post, sondern gilt entsprechend im herkömmlichen Briefverkehr. Ein Defekt des Briefkastens liegt im Risikobereich des Empfängers. Die Nachricht gilt als zugegangen, auch wenn vielleicht danach der Briefkasten abgebrannt ist und der Empfänger vom Inhalt gar nicht mehr Kenntnis nehmen konnte.

Während man jedoch das Fehlen oder die Zerstörung eines Hausbriefkastens gut erkennen kann, sind Fehler in einem elektronischen Postfach deutlich unauffälliger. Es scheint dringend geboten, das in entsprechenden Gesetzen und Verordnungen zu berücksichtigen, damit Bürger überhaupt eine Chance haben, rechtzeitig reagieren zu können.

Neben der Zustellung an sich kann deren Zeitpunkt vor allem für fristgebundene Willenserklärungen von erheblicher Bedeutung sein. Juristisch gilt eine Willenserklärung als zugegangen, wenn unter normalen Umständen mit deren Kenntnisnahme zu rechnen ist. So bewirkt das Einwerfen eines Briefes in den Postkasten einer Privatperson um 22:30 Uhr den Zugang erst am nächsten Tag. Entsprechendes gilt für elektronische Erklärungen. Auch in diesem Bereich könnte De-Mail, flankiert von gesetzlichen Zugangsregelungen, durch die Verwendung von Versand- und Empfangsbestätigungen mit Zeitstempeln zu einer deutlichen Steigerung der Rechtssicherheit führen.

Der Empfänger muss allerdings seine Empfangseinrichtung, also auch sein E-Mail-Postfach, überhaupt erst einmal dem Empfang von rechtsgeschäftlichen Nachrichten gewidmet haben, bevor dort jemand etwas rechtsgültig zustellen kann. Während dies beim normalen Briefkasten im Allgemeinen angenommen wird, muss sich bei einem E-Mail-Postfach der Widmungswille ausdrücklich oder aus dem Zusammenhang ergeben, etwa durch Angabe der E-Mail-Adresse auf einem Briefkopf des Unternehmers oder durch ausdrückliche Erklärung gegenüber einem Vertragspartner. Auch hier könnte die Einrichtung von De-Mail-Accounts die Rechtssicherheit erhöhen, indem man etwa gesetzlich normiert, dass De-Mail-Adressen allgemein dem Empfang von Erklärungen aller Art gewidmet sind. In diesem Fall würde die Speicherung einer Nachricht in einem zertifizierten E-Mail-Account den rechtssicheren Zugang bewirken. Ob der Nutzer die Möglichkeit erhält, die Widmung einzuschränken oder vollständig aufzuheben, bleibt eine Frage der konkreten gesetzlichen Gestaltung.

Verlässliche elektronische Welt?

Auch der Missbrauch von Nutzeraccounts hat erhebliche Auswirkungen auf das Vertrauen der Nutzer in den E-Commerce. Die Urheberschaft von Erklärungen lässt sich im Internet zurzeit nur mit großem Aufwand oder überhaupt nicht nachweisen. Nach den allgemeinen Regeln des Vertragsschlusses und des Beweisrechts gilt aber, dass der anspruchstellende Vertragspartner beweisen muss, dass eine Person ein Angebot abgegeben hat oder einen Vertrag unter einem Nutzeraccount (beispielsweise bei Ebay) angenommen hat. Das kann er zurzeit praktisch nicht.

Nach einhelliger Rechtsprechung spricht auch kein Anscheinsbeweis, also die Beweisführung auf Grundlage

Onlinequellen

[a] Dokumentation zur De-Mail und zu den Bürgerportalen
www.de-mail.de

[b] E-Government-2.0-Programm der Bundesregierung
www.kbst.bund.de/Content/Egov/Initiativen/EGov2/EGov2.html

[c] Initiative i2010
ec.europa.eu/information_society/eeurope/i2010/index_en.htm

[d] IT-Gipfel der Bundesregierung
www.cebit.de/it_gipfel_d

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

eines typischen Geschehensablaufes, zu seinen Gunsten, solange reine Benutzername-/Passwort-Systeme der Authentifizierung dienen. Das dürfte auch für Erklärungen gelten, die unter Verwendung des Authentifizierungsniveaus „normal“ im Rahmen von Bürgerportalen zustande kommen. Kommunikation über De-Mail-Accounts unter Verwendung der Niveaus „hoch“ und „sehr hoch“ kann aber möglicherweise mehr Rechtssicherheit gewährleisten, da in diesen Fällen vermutlich auch ein Anscheinsbeweis für die Urheberschaft der Erklärung gesetzlich verankert oder zumindest von der Rechtsprechung angenommen werden wird. Den größten Zuwachs an Rechtssicherheit brächte sicherlich eine gesetzliche Regelung. Ob dies in allen Fällen sinnvoll ist, wird sich zeigen.

Noch mehr Gesetze

Das Bundesministerium des Inneren geht davon aus, dass die Umsetzung der Bürgerportale zunächst ein Bürgerportalgesetz erfordert. Dessen Kernstück bilden die Anforderungen an Anbieter, Haftungsklauseln und Deckungsvorsorge, die Regelung der notwendigen zuverlässigen Erstregistrierung und die Beleihung der Diensteanbieter – also die Ausstattung mit Hoheitsrechten für einen bestimmten Aufgabenbereich – mit Hoheitsbefugnissen für die förmliche Zustellung. Hinzu kommen Regelungen für den Fall des Ausfalls eines Diensteanbieters, zur Sperrung von Accounts sowie der Zuständigkeit für den Bereich der Aufsicht.

Daneben wird für E-Government-Anwendungen die Änderung des Verwaltungsverfahrensgesetzes zur automatischen Zugangseröffnung erforderlich sein. Außerdem sollen De-Mail-Adressen Eingang in das Bundesmeldegesetz finden. Im E-Commerce sind darüber hinaus Ergänzungen und Änderungen vor allem der Zivilprozessordnung wünschenswert. Denkbar ist auch die Einführung einer förmlichen Zustellbestätigung in Anlehnung an § 182 ZPO. Dafür wäre die Beleihung des BPDA unabdingbar.

Aktueller Stand

Seit dem Jahr 2007 existieren die Konzepte für die De-Mail-Basisdienste (Postfach und Versand, Authentifizierung und Dokumentensafe) und für das Zertifizierungsverfahren. Nach einer Marktanalyse mit Unternehmen der Privatwirtschaft soll im weiteren Verlauf des Jahres 2008 die Feinkonzeption des Zertifizierungsverfahrens, die Pilotierung erster Bürgerportale sowie die Schaffung rechtlicher und organisatorischer Grundlagen für den Onlinebetrieb erfolgen. Schließlich sollen nach aktueller Planung die ersten Bürgerportale ab der zweiten Jahreshälfte 2009 online gehen. In den kommenden Jahren sollen Erkenntnisse aus dem Pilotbetrieb in die Konzeption und das Zertifizierungsverfahren einfließen.

Fazit

Der Erfolg der Bürgerportale und insbesondere der De-Mail steht und fällt mit der Beteiligung der Bürger – und damit das Geschäftsmodell der BPDAs. Es wird sich zeigen, ob es möglicherweise gar zu einem schleichenden Zwang zur Nutzung von De-Mail kommt, etwa durch den Versand der Steuerbescheinigung per De-Mail. Unabhängig von dieser Fragestellung soll die Einführung von Bürgerportalen zu mehr Rechtssicherheit im E-Commerce und E-Government führen und damit letztendlich Vorteile für den Bürger bringen. Ob sie mögliche Nachteile aufwiegen werden, lässt sich noch nicht absehen. Jede Form von Sicherheit ist besser als gar keine Sicherheit; dennoch sollten nicht die rechtlichen Regelungen allein das Maß der Dinge bilden. Man darf daher schon gespannt sein, welche Funktionen und Sicherheitsmerkmale die ersten Prototypen bieten werden. (un)

CHRISTOPH WEGENER

CISA, CISM und CBP, ist promovierter Physiker und mit der wecon.it-consulting freiberuflich mit IT-Sicherheit befasst. Zudem ist er Gründungs- und Vorstandsmitglied der Arbeitsgruppe Identitätsschutz im Internet (a-i3).

DENNIS WERNER

ist Rechtsanwalt mit dem Interessenschwerpunkt IT-Recht in der Hagener Kanzlei Dr. Kleffmann & Partner GbR und Gründungs- und Vorstandsmitglied der Arbeitsgruppe Identitätsschutz im Internet (a-i3) e. V.





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Marktübersicht: PC-Managementsoftware

Turnschuhe ade

Nils Kaczenski

Komplexe unternehmensweite Netzstrukturen und aufwendige Softwareinstallation mit differenzierten Anpassungen erfordern – um das Ganze am Laufen zu halten – einen hohen Aufwand vom IT-Personal. Sollte man da nicht beizeiten über eine Automatisierung nachdenken? Die Darstellung von Kriterien für diesen Prozess und eine Marktübersicht relevanter Produkte erleichtern den Einstieg in das PC-Management.

Selbst in mittelständischen Unternehmen trifft man noch erstaunlich oft das klassische „Management by Sneaker“ an: Jeder Rechner im Netzwerk ist dabei ein Unikat und bedarf individueller Betreuung. So ist das IT-Personal buchstäblich viel unterwegs, um PCs zu installieren, zu konfigurieren oder im Zweifel komplett neu aufzusetzen. Manche behelfen sich dabei mit einer Teillösung und nutzen Software für den Fernzugriff. Bordmittel oder frei verfügbare Tools lassen aber Notwendiges vermissen. Aber auch wenn es remote klappt, bleibt der Umstand, dass PCs in diesen Netzen individuell behandelt werden.

Da der Aufwand, der durch diese simple Methodik entsteht, selten in einem sinnvollen Verhältnis zum Nutzen steht, hat sich ein umfangreicher Anbietermarkt mit Werkzeugen zum Client-Management gebildet. Wie kommt es dann aber, dass in mittelständischen Unternehmen und selbst im gehobenen Segment der Enterprise-Netzwerke viele IT-Abteilungen auf die Chance der Automatisierung und Zentralisierung verzichten?

Ein Grund sind sicher die hohen Investitionen. Ein Softwaresystem einzuführen, das die Installations- und Wartungsprozesse im Rechnerpark vereinfacht, ist zunächst mit Kosten verbunden, die im laufenden Budget kaum zu verstecken sind. Und selbst wenn ein solches Werkzeug erstanden wurde, braucht es eine bedeutende Anstrengung, es in Betrieb zu setzen: Admins müssen den Bedarf analysieren, eine Client-Software ausrollen, eine Ist-Aufnahme durchführen und Pakete schnüren. Dazu kommt der Einarbeitungsaufwand. Und das alles neben der laufenden Tätigkeit der IT-Abteilung, die ja selbst schon so ausgeufert ist, dass man sie eigentlich reduzieren wollte.

Von der Einsicht zur Umsetzung

Kaum verwunderlich, dass viele sich scheuen und dass viele der Produkte als „Schrankware“ enden: Man beschafft sie, setzt sie aber nicht ein, weil man das Projekt so lange vor sich herschiebt, bis es sinnlos geworden ist. Zudem gibt es noch einen psychologischen Faktor: Nicht wenige Administratoren fürchten, sich selbst oder ihre Kollegen mit einer Client-Managementsoftware überflüssig zu machen, haben die Hersteller dieser Software

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

doch unisono die Senkung der IT-Kosten in ihre Hochglanzbroschüren geschrieben. Meist dürften solche Befürchtungen unbegründet sein, denn der Aufwand für Betrieb und Pflege eines solchen Systems ist nicht zu unterschätzen – dafür läuft es aber auf höherem Niveau.

Widerstand ist nicht zu unterschätzen

Die Argumente für den Einsatz eines Client-Managements sind durchaus vielfältig. Einmal eingeführt, können solche Werkzeuge den Gesamtaufwand für die Pflege der IT-Landschaft drastisch verringern. Ein fertiges Softwarepaket auszurollen, erfordert nicht mehr, als es dem Zielrechner zuzuweisen. Meist geschieht das über Konstrukte wie Computergruppen oder Arbeitsplatzprofile, verbreitet sind Regelwerke, die die Pakete anhand von Eigenschaften der Rechner oder Benutzerobjekte zuordnen.

Das zweite klassische Element einer solchen Verwaltungs-Suite ist die Inventarisierung, die den nötigen Überblick über den Gerätepark schafft und, wenn sie gut gemacht ist, flexible Abfragemöglichkeiten eröffnet. Das Ergebnis einer Inventarabfrage lässt sich direkt als Kriterium für die Softwareverteilung nutzen. Vor Migrationen oder der Einführung einer neuen zentralen Applikation liefert die Bestandsdatenbank die nötigen Informationen, um die Eignung der Clients bewerten zu können.

Ein weiterer Bestandteil der Suiten ist die Fernzugriffsfunktion auf Arbeitsplatzrechner – seit XP-Zeiten in einfacher Form Bestandteil der Betriebssysteme. Will man diese Zugriffe komfortabler ansteuern oder muss man Mac- und Linux-Rechner mit einbeziehen, wird die Sache komplizierter; dann reichen die Bordmittel nicht mehr. So oder so sollte der Administrator die Datenschutzaspekte beachten und sich vor dem „Aufschalten“ das Einverständnis des Anwenders einholen.

Neben den Kernfunktionen, die die Administrationskosten der Clients reduzieren, kommt ein weiterer Faktor ins Spiel: die Erhöhung der Qualität. Ein validiertes Paket oder ein gut getesteter automatischer Prozess vermeidet Fehler, die sich in der manuellen Massenarbeit sonst einschleichen können. So kann man keine Softwarekomponente vergessen und definierte Standards erfüllen. Nicht nur Eigenentwicklungen, auch kommerzielle Software setzen bisweilen Zusatzkomponenten voraus, etwa einen bestimmten Datenbank-Client oder eine Laufzeitumgebung wie Java oder .Net. Abhängigkeiten dieser Art sollte ein Regelwerk innerhalb der Softwareverteilung auflösen können. Wenn es darauf ankommt, eine Anwendung zu einem vorgegebenen Zeitpunkt verfügbar zu haben, kommt man an einer programmgesteuerten Verteilung kaum vorbei.

Wer braucht welche Informationen

Für Daten über die Ausstattung der IT-Infrastruktur interessieren sich ganz unterschiedliche Stellen des Unternehmens. Während das Operating auf aktuelle technische Informationen mit großer Detailtiefe angewiesen ist, braucht die Buchhaltung kaufmännische Daten, zum Beispiel die Information, welches Softwareprodukt wie oft eingesetzt ist. Voraussetzung hierfür ist eine intelligente Inventardatenbank, die gleichartige Software auch dann erkennt, wenn sie mit unterschiedlichen Bezeichnungen daherkommt und umgekehrt Varianten auseinanderhalten kann, wenn dies lizenzrechtlich notwendig ist. Ob Reports von Softwareherstellern als Nachweis der korrekten Lizenzierung akzeptiert werden, muss man im Einzelfall erfragen. Eine Zertifizierung derartiger Auswertungen gibt es jedenfalls nicht.

Apropos Reports: Da Inventardaten aus unterschiedlicher Sicht von Interesse sind, kann ein Werkzeug von Vorteil sein, das flexible Zugänge zu den Informationen ermöglicht. Den IT-Leiter interessieren vielleicht nur Zusammenfassungen im Ampelformat – grün für „alles okay“, rot für „hier muss was passieren“. Der Geschäftsführer will wissen, ob er die vorhandenen Gerätschaften wirklich schon erneuern muss, und der Windows-Admin will den Rollout-Prozess des letzten Service-Packs kontrollieren. Wer diese Anforderungen hat, sollte auf dynamische Berichte Wert legen, die je nach Rolle vordefiniert oder flexibel konfigurierbar sein sollten. Interessant kann eine Historienfunktion sein. Sie könnte

Office-Stolperfalle

Nicht nur Vista hat neue Techniken mitgebracht, sondern auch die am häufigsten darauf aufsetzende Applikations-Suite. Mit Office 2007 hat Microsoft ein neues Installationsformat eingeführt, das in zentralen Punkten anders funktioniert als seine Vorgänger. Anpassungen werden genau wie Updates als Patches (*.*msp*) behandelt und nicht mehr in einer eigenen Template-Datei (*.*mst*) abgelegt. Als Folge scheitern die bisherigen Verteilungstechniken, die mit *.mst*-Dateien arbeiten. So kann man beispielsweise keine angepasste Installation von Office 2007 mit den Windows-eigenen Gruppenrichtlinien ausführen.

Da Microsoft Office 2007 noch dazu veröffentlicht hat, bevor die neue MSI-Spezifikation bekannt war, hatten viele Hersteller von Softwareverteilungen ein echtes Problem. Ihre Setup-Mechanismen scheiterten an dem neuen Format. Hinzu kommen einige Ungereimtheiten bei MSI im Allgemeinen und beim Office-Paket im Speziellen, sodass es bei manchen Anbietern immer noch etwas knirschen kann. Mittlerweile behaupten aber alle, diese Dinge im Griff zu haben.

iX-TRACT

- PC-Managementsoftware soll die Verwaltung ganzer IT-Landschaften zentralisieren und automatisieren.
- Dabei deckt sie den Lebenszyklus der Arbeitsplatzrechner, der Netzinfrastruktur sowie der Betriebssystem- und Softwareinstallation ab.
- Über viele Jahre hat sich ein Markt entwickelt, in dem sowohl große, weltweit operierende Softwarehersteller als auch kleinere, regional tätige Anbieter ihre Produkte anbieten.
- Unter den Management-Suiten gibt es Generalisten, die versuchen das Aufgabengebiet vollständig abzudecken, und – gerade im Security-Segment – Spezialanwendungen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

zum Beispiel zeigen, dass nach dem Wochenende die RAM-Ausstattung eines Rechners plötzlich geringer ist, weil jemand einen Speicherriegel hat mitgehen lassen.

Sicherheit durch Automatisierung

Wer für die Netzwerksicherheit verantwortlich ist, findet im Client-Management ebenfalls Unterstützung. Das beginnt bei Fragen wie den lokalen Administratorrechten, die die Installation von Software meist voraussetzt. Hier arbeiten fast alle Systeme mit eigenen Diensten, die das Einrichten der Pakete übernehmen und vom Benutzer keine erhöhten Berechtigungen fordern. Das kann so weit gehen, dass ad hoc angestöpselte Hardware für den Benutzer nutzbar wird, wenn das System einen freigegebenen Treiber selbsttätig installieren kann. Von grundsätzlicher Bedeutung für die allgemeine Betriebs- und Zugriffssicherheit sind definierte Umgebungen. Nur ein bekannter Satz von Programmen wird auf die Clients losgelassen, am besten rollenbasiert nach Anwender. Nicht autorisierte Programme bleiben somit außen vor.

Wesentlich weiter geht dabei eine Klasse von Managementsystemen, die erst seit wenigen Jahren am Markt vertreten ist. Sie segeln unter der Flagge „Endpoint Security“ und bieten an, den Arbeitsplatzrechner und das Verhalten des Anwenders wesentlich feiner abgestuft zu steuern als das Betriebssystem selbst es vorsieht. Die Applikationskontrolle prüft beispielsweise, ob ein gestartetes Programm für den Anwender wirklich zugelassen ist. Das geht weiter als die Softwareverteilung, denn wenn diese einmal ein Paket installiert hat, ist es in der Regel auch ausführbar. Die Prüfung solcher Binaries erfolgt nach verschiedenen Kriterien, etwa anhand des Speicherpfades, des eingetragenen Besitzers oder auch über Hash-Werte der Programmdatei. Die Kehrseite der Medaille besteht im erhöhten Verwaltungsaufwand für die Berechtigungsverwaltung.

Es gibt Werkzeuge, die nicht nur das ausgeführte Programm überprüfen, sondern auch einzelne Programmfunktionen kontrollieren. Technische Ansätze reichen hier vom Ausblenden von Menüoptionen bis zur Überwachung, was das Programm eigentlich gerade macht. Nicht immer bleibt dies ohne Auswirkungen auf die Performance und es kann zudem – wegen der möglichen Überwachung der Mitarbeiter – datenschutzrechtliche Fragen tangieren.

Ähnliche Schwachstellen analysieren Gerätewächter, die den Zugriff auf externe oder interne Speicher oder andere I/O-Geräte steuern. Der Besorgnis, dass Mitarbeiter sensible Daten auf einfache USB-Sticks oder ihren iPod kopieren und aus dem Unternehmen schleusen, kann man so entgegentreten. Hier lassen Betriebssysteme viele Lücken, auch wenn Vista grundlegende Mechanismen mitbringt darauf zu reagieren. Spannend wird es aber, wenn man den Zugriff nicht einfach absolut verbieten, sondern situationsgerecht steuern möchte: Nicht jedes externe Speichermedium ist böse, es kann sich ja um Daten handeln, die der Anwender dringend benötigt.

Obwohl es sich hierbei durchaus um Aufgaben handelt, die man dem klassischen Client-Management zurechnen kann, gibt es häufig eine Zweiteilung am Markt: So konzentrieren sie einige Hersteller ausschließlich auf diese Endpoint Security, während andere nur den klassischen Dreiklang Softwareverteilung, Inventarisierung und Fernzugriff bieten.

Pakete schnüren und verschicken

In der Softwareverteilung können alle Hersteller laut eigenen Angaben mit den neuen Mechanismen von Vista und Office 2007 umgehen. Ebenso geben alle an, dass auch Benutzer ohne Administratorrechte Anwendungen und Treiber installieren können und detaillierte Logs über das Setup zu führen. Hier und bei weiteren Features wie dem Aufbau von Workflows und komplexen Installationen aus Softwarepaketen oder der Einbindung mobiler Nutzer sollten Interessenten aber genau hinschauen. Während manche Werkzeuge eigene Paketierungsprogramme mitbringen, die über Regeln oder Skriptsprachen komplexe

Vista-Installation

Microsofts jüngste Generation von Client-Software scheint, trotz teils jahrelanger Beta-Phasen, viele Hersteller völlig unvorbereitet getroffen zu haben. In der Tat hat man in Redmond gerade für die automatisierte Installation einen Großteil seiner bisherigen Ansätze über Bord geworfen und neue Mechanismen geschaffen.

Das fängt beim Datenträger an. Er enthält nicht mehr die komprimierten Einzeldateien, die das Betriebssystem ergeben, sondern ein großes Image, in dem alles Nötige enthalten ist. Damit nicht genug, hat Microsoft gleich ein neues Imageformat eingeführt, das nicht wie bei den meisten Drittanbietern sektorbasiert arbeitet, sondern dateibasiert aufgebaut ist. Damit umgeht man mögliche Probleme bei der Festplattengeometrie und ermöglicht gleichzeitig die Ablage mehrerer Varianten im selben Image. Eine integrierte Steuerdatei legt fest, welche Dateien zu welcher Version gehören. So liefert eine Standard-DVD alle Editionen von Vista aus, erst der Setup-Key entscheidet, was auf der Festplatte landet.

Um mit der neuen Technik umgehen zu können, liefert Redmond einen eigenen Satz an Werkzeugen, die individuelle und automatisierte Installationen zulassen. Dazu gehören etwa ein Komponentenmanager, der die Steuerdateien für die Installation bearbeitet, oder Tools, die das Image manipulieren oder ergänzen. Das bedeutet aber gleichzeitig, dass viele Werkzeuge von Drittanbietern plötzlich nicht mehr funktionieren. Hinzu kommt, dass das zu 2000- oder XP-Zeiten erworbene Know-how überholt oder zumindest ergänzungsbedürftig ist, denn nicht nur die Formate, sondern die Philosophie hat sich deutlich geändert.

Da zumindest bei neuer Hardware zunehmend die 64-Bit-Variante eingesetzt wird, hat die klassische DOS-Bootdiskette ausgedient. Der Ersatz ist Windows PE (Pre-Execution Environment), eine Art abgespecktes Windows, das nur zum Einrichten oder Reparieren einer Windows-Installation gedacht ist. Es bildet die Grundlage des Setup-Programms auf der Vista-CD. Diese Software lässt sich für verschiedene Zwecke anpassen und von einem Datenträger oder über das per Netz ausführen.

Obwohl Microsoft eine Reihe von Werkzeugen selbst liefert, bleibt hier erheblicher Spielraum für Drittanbieter, denn Bordmittel sind oft kein Musterbeispiel an Integration. Um hier eine skalierbare und nutzbare Umgebung für ein größeres Netz zu schaffen, ist einiger Aufwand nötig. Die Produkte, die eine Betriebssysteminstallation durchführen, kommen heute mit den 64-Bit-Versionen von Vista klar, auch wenn nicht alle Hersteller die neue Image-Installation von Microsoft übernommen haben.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Marktübersicht: PC-Managementsoftware

Hersteller	Aagon Consulting	Baramundi Software	CA	DeskCenter Solution	FrontRange Solution	HP
Herstellerinformationen	sales@aagon.com	request@baramundi.de	cainfo.germany@ca.com	m.deuntzsch@deskcenter-solutions.net	sales@frontrange.com	www.hp.com
Name der Suite	ACMP Suite	Management Suite	Unicenter	Management Suite	Enteo Client Suite	Client Automation
aktuelle Version/erste Version im Jahr	3.5/2001	7.6.1/1998	11.2/k. A.	8.0.1/2004	6SR2/1997	7.2/1990
verfügbare Sprachen (deutsch/englisch/weitere)	✓/✓/–	✓/✓/✓	✓/✓/–	✓/✓/–	✓/✓/–	✓/✓/✓
benötigte Infrastruktur	ab Win2k+SQL2k	ab Win2k+SQL2k	ab Win2k+SQL2k	ab Win2k+SQL2k	ab Win2k+SQL2k	diverse [7]
Einbindung anderer Managementsysteme	–	–	✓	✓	✓	✓
Unterstützung älterer Win-Vers./XP/Vista/Linux/Mac	✓/✓/✓/–/–	✓/✓/✓/–/–	k. A./✓/✓/✓/–	✓/✓/✓/–/–	✓/✓/✓/–/–	k. A./✓/✓/✓/–
Betriebssysteminstallation						
installiert ältere Win-Vers./XP/Vista/Linux/Mac	✓/✓/✓/–/–	✓/✓/✓/–/–	k. A./✓/✓/✓/–	✓/✓/✓/–/–	✓/✓/✓/✓/–	✓/✓/✓/✓/✓
unterstützt 64-Bit-Systeme	✓	✓	✓	✓	✓	✓
über WIM-Format/eigenes Paketformat	–/✓	–/✓	✓/✓	✓/–	✓/✓	✓/–
über Netzwerk automatisch/anpassbar	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
über Medium automatisch/anpassbar	–/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Anpassung nachträglich möglich	✓	✓	✓	✓	✓	✓
Softwareverteilung						
unterstützt MSI/eigenes Packaging-Werkzeug	✓/✓	✓/✓	✓/✓	✓/–	✓/✓	✓/✓
detaillierte Logs über die Installationen	✓	✓	✓	✓	✓	✓
Softwarepakete modular kombinierbar	✓	✓	✓	✓	✓	✓
unterstützt mobile Nutzer	k. A.	✓	✓	✓	✓	✓
Application Streaming						
Sandboxing für gestreamte Applikationen	✓	–	–	✓	–	✓
Datenaustausch zwischen gestreamten Applikationen	✓	–	–	✓	✓	✓
gestreamte Applikationen offline verfügbar	✓	–	–	✓	✓	✓
Inventarisierung						
inventarisiert Software/Hardware/Lizenzen	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓
Reporting über Lizenznutzung	✓	✓	✓	✓	✓	✓
beinhaltet Historienfunktion/Inventarliste erweiterbar	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
kann Inventar für Softwareverteilung nutzen	✓	✓	✓	✓	✓	✓
Patch-Management						
unterstützt Microsoft-Update/weiteres Verfahren	–/k. A.	–/✓	–/✓	✓/–	✓/–	✓/✓
Patch-Management ist Teil der Softwareverteilung	✓	✓	✓	✓	✓	✓
differenzierte Freigabe/Locking	✓/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Clients auf ihren Patch-Status untersuchen	✓	✓	✓	✓	✓	✓
Management von Benutzerprofilen						
Anpassung zwischen Betriebssystem-/Applikationsversionen	✓/k. A.	–/–	–/–	–/–	✓/✓	✓/✓
verwaltet mehrere Profile auf demselben Rechner	✓	✓	–	–	✓	✓
konvertiert lokale und servergespeicherte Profile	k. A.	–	–	–	–	–
Bereinigen von Profilen möglich	k. A.	✓	–	–	✓	✓
Fernzugriff auf Clients						
übermittelt ganzen Bildschirm/Bereiche des Bildschirms	✓/✓	✓/–	✓/–	✓/–	✓/✓	✓/–
Dateiübertragung auf den Client	✓	–	✓	✓	✓	–
Authentisierung des Supportmitarbeiters	✓	–	✓	✓	✓	✓
Zustimmungsoption für den Benutzer	✓	✓	✓	✓	✓	✓
Aufzeichnung einer Session	–	k. A.	✓	–	✓	–
Steuerung des Applikationszugriffs						
Identifizieren der Applikation über Name/Hash/Zertifikat	✓/–/–	–/–/–	–/–/–	–/–/–	–/–/–	–/–/– [3]
Sperrung einzelner Programmfunktionen	–	–	–	–	–	– [3]
Zugriffssteuerung über Whitelist/Blacklist	–	–/–	–/–	–/–	–/–	–/– [3]
bei Verweigerung eigene/Standard-Fehlermeldung	–/✓	–/–	–/–	–/–	–/–	–/– [3]
Logging von Zugriffen und Zugriffsversuchen	–	–	–	–	–	– [3]
zeitgesteuerter Zugriff/Unterstützung mobiler Benutzer	–	–/–	–/–	–/–	–/–	–/– [3]
Steuerung von Gerätezugriffen						
Geräte bzw. Geräteklassen	–	–	–	–	✓ [6]	✓ [4]
Zugriffssteuerung über Whitelist/Blacklist	–/–	–/–	–/–	–/–	✓/✓	–
bei Verweigerung eigene/Standard-Fehlermeldung	–/–	–/–	–/–	–/–	✓/✓	–/✓
Logging von Zugriffen und Zugriffsversuchen	–	–	–	–	✓	✓
zeitgesteuerter Zugriff/Unterstützung mobiler Benutzer	–/–	–/–	–/–	–/–	✓/✓	–/✓
Erkennen von Sicherheitsproblemen						
Discovery-Funktion für Netzwerkhardware	✓	–	–	–	–	✓
Betrieb mit Agenten/ohne Agenten	✓/✓	–/–	–/–	–/–	–/–	✓/✓
Reporting über Netzstatus	–	–	–	–	–	✓
Benachrichtigung bei Problemen	✓	–	–	–	–	✓
automatisches Beheben	✓	–	–	–	–	✓
Daten-/Laufwerksverschlüsselung						
einzelne Dateien und Ordner auf dem Client/Server	–/–	–/–	–/–	–/–	–/–	–/–
von Festplatten/Wechselmedien	–/–	–/–	–/–	–/–	–/–	–/–
für mehrere Benutzer/Windows-Gruppen	–/–	–/–	–/–	–/–	–/–	–/–
durch Administrator/Benutzer steuerbar	–/–	–/–	–/–	–/–	–/–	–/–

[1] nur Sicherheitsprofile für Benutzer und Computer; [2] Schnittstellen, Wireless Interfaces und Speichergeräte; [3] Steuerung geschieht über HP CA Policies. Hier lassen sich Benutzerapplikationszusammenhänge festlegen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Lumension Security	Materna	Matrix42	Microsoft	NetSupport	Novell	Symantec	Utimaco Safeware
www.lumension.de	marketing@materna.de	info@matrix42.de	www.microsoft.com	sale@pci-software.de	www.novell.com	www.altiris.com/sales/emea/germany.aspx	mirlinda.nuha@utimaco.de
Sanctuary[8]	DX-Union	Empirum	SCC Manager	DNA	ZENworks	Altiris Client Management Suite	SafeGuard Enterprise
4.3/2000	6.2/1989	2008AddOn2/2000	2007R2/k. A.	2.7/2003	10.1/2007	6.5/1998	5.3/2006
✓/✓/–	✓/✓/–	✓/✓/–	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓/
Win-/Unix-Server	Win-/Linux-Server	Win-/Linux-Server	ab Win2003+SQL2005	ab win2k+SQL2k	ab Win2003+SQL2005	ab win2k+SQL2k	ab Win2k+SQL2k
–	✓	✓	✓	✓	✓	✓	✓
✓/✓/✓/–/–	k. A./✓/✓/✓/–	✓/✓/✓/✓/–	k. A./✓/✓/✓/✓	✓/✓/✓/✓/–	✓/✓/✓/–/–	✓/✓/✓/–/–	✓/✓/✓/–/–
–/–/–/–/–	✓/✓/✓/✓/–	✓/✓/✓/✓/–	k. A./✓/✓/–/–	–/–/–/–/–	✓/✓/✓/–/–	✓/✓/✓/✓/✓	–/–/–/–/–
–	✓	✓	✓	–	✓	✓	–
–/–	✓/✓	✓/✓	✓/–	–/–	✓/✓	✓/✓	–/–
–/–	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓	–/–
–/–	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓	–/–
–	✓	✓	✓	–	✓	✓	–
–/–	✓/✓	✓/✓	✓/–	✓/✓	✓/✓	✓/✓	–/–
–	✓	✓	✓	✓	✓	✓	–
–	✓	✓	✓	✓	✓	✓	–
–	✓	✓	✓	–	✓	✓	–
–	✓	✓	✓	–	✓	–	–
–	k. A.	✓	✓	–	✓	✓	–
–	k. A.	✓	✓	–	✓	✓	–
–/–/–	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	–/–/–
–	✓	✓	✓	✓	✓	✓	–
–/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	–/–
–	✓	✓	✓	✓	✓	✓	–
–/✓	✓/✓	✓/–	✓/✓	–/–	–/✓	–/–	–/–
–	✓	✓	✓	–	✓	✓	–
✓/✓	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓	–/–
✓	✓	✓	✓	–	✓	✓	–
–/–	✓/✓	✓/✓	✓/✓	–/–	–/–	✓/✓	–/–
–	✓	✓	✓	–	–	✓	✓[1]
–	✓	✓	–	–	–	✓	–
–	✓	✓	–	–	–	✓	–
–/–	✓/–	✓/✓	✓/–	✓/✓	✓/–	✓/–	–/–
–	✓	✓	✓	✓	✓	✓	–
–	✓	✓	✓	✓	✓	✓	–
–	✓	✓	✓	✓	✓	✓	–
–	✓	✓	✓	✓	–	✓	–
✓/✓/–	✓/–/–	✓/✓/–	–/–/–	–/–/–	über Header	✓/–/–	–/–/–
–	–	✓	–	–	–	–	–
✓/✓	✓/–	✓/–	–/–	–/–	–/✓	✓/✓	–/–
✓/✓	✓/–	✓/✓	–/–	–/–	–/✓	✓/✓	–/–
✓	✓	✓	–	–	✓	✓	–
–/✓	–/✓	✓/✓	–/–	–/–	–/✓	✓/✓	–/–
✓[2]	alle	✓[2]	k. A.	k. A.	k. A.	✓[5]	✓[2]
✓/✓	✓/–	✓/✓	✓/✓	k. A./k. A.	✓/✓	✓/✓	✓/✓
✓/✓	✓/–	✓/✓	k. A./k. A.	✓/–	–/✓	✓/✓	✓/–
✓	✓	✓	k. A.	✓	✓	✓	✓
✓/✓	–/✓	✓/✓	–/✓	✓/–	–/✓	✓/✓	–/✓
✓	✓	✓	k. A.	–	–	✓	✓
–/✓	–/✓	✓/✓	k. A.	✓/–	–/–	✓/✓	✓/✓
✓	–	✓	k. A.	–	–	–	–
✓	–	✓	k. A.	–	–	✓	–
✓	–	✓	✓	✓	–	✓	–
✓/–	–/–	✓/✓	✓/✓	k. A./k. A.	✓/–	–/–	✓/✓
✓/✓	–/–	✓/✓	✓/–	k. A./k. A.	✓/✓	✓/✓	✓/✓
✓/✓	–/–	✓/✓	✓/–	k. A./k. A.	✓/✓	✓/✓	✓/✓
✓/✓	–/–	✓/✓	✓/✓	✓/k. A.	✓/✓	✓/–	✓/✓

[4] über BIOS-Einträge – eingeschränkt auf HP-Hardware; [5] Laufwerke und Ports; [6] USB und CD Devices; [7] Windows oder Unix, immanente und beliebige externe Datenbank; [8] einschließlich Patchlink VMS

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Angaben in der Marktübersicht

Die Tabelleneinträge der Marktübersicht basieren auf Herstellerangaben. Leider fehlt ein wichtiges Produkt, nämlich Tivoli von IBM. Der Hersteller sah sich nicht in der Lage (Urlaubszeit und Überlastung), den zugegebenermaßen umfangreichen Fragebogen auszufüllen.

Die Angaben in der Tabelle basieren auf einem relativ groben Raster. Hinter den Haken verbergen sich oft Informationen, die im Detail durchaus mehrere Absätze oder Seiten lang sind und hinter Strichen oft Relativierungen, dass es vielleicht über Skripte doch zu realisieren wäre oder dass man eben aufgrund des offenen Konzeptes andere Produkte einbinden kann. PC-Managementsoftware ist so komplex, wie die Anwendungsfälle individuell und vielschichtig sind. Insofern kann die Marktübersicht nur ein erster Einstieg sein.

Abläufe zulassen, verteilen andere nur fertige Pakete. In diesem Fall benötigt der Administrator ein externes Paketierungsprogramm und ist damit auf dessen Fertigkeiten angewiesen.

Das ist bei manchen „Home-grown Applications“ relevant, die etwa zunächst den Datenbank-Client, dann ein Runtime-Framework, schließlich die Applikation selbst und abschließend diverse Anpassungen benötigen. Wer solche Aufgaben zu erfüllen hat, tut gut daran, vor der Auswahl einen genauen Blick auf die Paketierungs- und Zuweisungsmechanismen der Kandidaten zu werfen, denn hier unterscheiden sie sich teils deutlich.

Sandkastenspiele: Pflanzen und pflegen

Der Zugriff für mobile Benutzer wird zwar von allen unterstützt, real aber wenig einheitlich durchgeführt. Einige Programme bieten methodische Freiheit mit Offline-Verteilung, Installation von Medien oder ausgefeilter Bandbreitensteuerung. Andere benötigen stets Kontakt zum Verteilserver oder lassen solche Szenarien nur mittels aufwendig angepasster Skripte zu.

Das Betriebssystem-Deployment gehört nicht bei allen Anbietern zum Standardprogramm. Hier besteht in den Unternehmen zudem oft wenig Bedarf, weil die eigene IT-Abteilung gute Erfahrungen mit Image-Rollouts gemacht hat. Insbesondere im Fall von Vista liegt dies auch nahe. Für das Patch-Management bietet Microsoft selbst mit den WSUS (Windows Server Update Services) ein mittlerweile recht ausgereiftes und kostenloses Tool an. Seine Mechanismen dienen den meisten Anbietern als Grundlage ihrer eigenen Systeme.

In diesem Segment unterscheiden sich die Mitbewerber teils deutlich voneinander: Manche bieten Mehrwerte durch die Integration von Patches anderer Hersteller oder durch bessere Kontroll- oder Zuweisungsfunktionen. Wirklichen Zusatznutzen kann ein Reporting über ausgerollte Patches oder den Ist-Zustand eines Clients ergeben. Hier öffnet sich die Schnittstelle zur Schwachstellenanalyse (neudeutsch: Vulnerability-Management) der Endpoint-Security-Fraktion.

Management von Virtualisierungen

Ein relativ neues Thema verbirgt sich hinter dem Begriff „Application Streaming“, auch als „Applikationsvirtualisierung“ bekannt. Beide Bezeichnungen sind nicht ganz korrekt, denn im Wesentlichen geht es darum, sich die lokale Installation einer Anwendung mit all ihren Abhängigkeiten zu sparen. Systeme dieser Art fassen Applikationen mitsamt der nötigen Umgebung wie Runtime-Komponenten, Registry-Einträgen oder Schnittstellen zu einem Gesamtpaket zusammen und führen sie über einen eigenen Client auf dem lokalen Rechner aus. Der Vorteil: Die Anwendung befindet sich in einer definierten und abgeschirmten „Sandbox“, die nicht mit anderen in Konflikt gerät und keine Rückstände auf dem System hinterlässt. Anders als bei Terminalservern steht die gesamte Leistung des Arbeitsplatzrechners zur Verfügung.

Die Idee selbst ist nicht neu. Bereits vor vielen Jahren gab es erste Programme, die solche Funktionen im Einzelfall bereitstellten. Die aktuelle Ausprägung geht aber weiter, weil sie zusätzliche Intelligenz und ausgereifte Managementfunktionen hinzufügt. Die Streaming-Idee etwa kommt zum Tragen, wenn der Server nur die Teile einer großen Applikation zum Client überträgt, die dieser gerade braucht. Berechtigungssteuerungen regeln auch hier, wer welche Applikation nutzen kann. Einige Hersteller integrieren solche Systeme in ihre Client-Management-Suiten. Bei manchen handelt es sich um Eigenentwicklungen, andere setzen OEM-Versionen von Drittherstellern ein.

Fazit

Die Markterhebung konnte nur einige klassische Funktionen des Management und einige wenige Werkzeuge der Endpoint Security berücksichtigen. Daneben gibt es eine große Zahl Antiviren-Softwarehersteller und Anbieter von Client Firewalls oder ähnlicher Tools, die ebenfalls ausgeblendet wurden.

Wie dieser Überblick und die Tabelle im Anschluss zeigen, tummeln sich unterschiedliche Ansätze auf dem großen Markt des Client-Management. Obwohl viele Hersteller eine vergleichbare gemeinsame Grundlage an Funktionen und Modulen haben, ist der Markt doch erheblich fragmentiert. So teilt sich das Feld praktisch in Management- und Sicherheitsanbieter. Zudem besteht eine stark ausgeprägte Regionalisierung. Neben einigen internationalen Platzhirschen wie HP, CA, Symantec oder Microsoft (und die hier nicht vertretene IBM) gibt es viele kleinere Hersteller, die nur lokale Bedeutung haben. In den europäischen Nachbarländern oder den USA hingegen findet man ein vergleichbares Feld von lokalen Anbietern, die hier praktisch unbekannt sind.

Die eierlegende Wollmilchsau, die alles kann, mag für viele nicht infrage kommen, weil sie manche Aufgaben vielleicht gut, aber nicht in der gewünschten Form löst, und weil sie relativ teuer ist. Hingegen mag ein Programm, dessen Featureliste überschaubar wirkt, genau den Bedarf treffen. Der Kunde hat die Qual der Wahl und sollte sich auf diese vorbereiten, indem er eine genaue Analyse des Ist-Zustandes seiner IT-Landschaft vornimmt und eine Vorstellung vom gewünschten Soll-Zustand entwickelt. Erst danach sollte er Vertreter möglicher Anbieter zum Kaffee einladen. (WM)

NILS KACZENSKI

leitet Consulting und Support bei der WITcom by Wahl GmbH + Co KG, Hannover.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Jubiläum: 25 Jahre GNU-Projekt

Sternzeichen GNU

Jon „Maddog" Hall, Peter Salus



Es gibt in der IT kaum jemanden, der mehr polarisiert als Richard Stallman. Die Geschichte der GNU-Projekts ist sehr eng mit seiner Person verwoben. Zwei „alte" IT-Kämpen beleuchten aus ihrer Sicht Stationen einer Entstehungsgeschichte.

Es war im Sommer 1969. Maddog hatte im vergangenen Sommer in einem Fernkurs FORTRAN gelernt und dies in seinem Nebenjob bei der Western Electric Plant in Baltimore, Maryland, auf einer IBM 1130 auch praktiziert. Nun war er wieder zurück an der Drexel-Universität in Philadelphia. Dort befanden sich die einzigen Computer, auf denen er seine elektronischen Simulationsprogramme laufen lassen konnte – hinter verschlossenen Türen.

Zu jener Zeit war Software außerordentlich teuer. Der Kauf einer einzelnen Kopie eines Compilers für FORTRAN oder COBOL (ja, die Namen schrieben sich versal, vielen Dank) konnte leicht 100 000 US-Dollar verschlingen – und das zu einer Zeit, als 100 000 US-Dollar noch richtig viel Geld waren. Als Student konnte sich Maddog das natürlich nicht leisten.

Glücklicherweise gab es die 1961 gegründete Digital Equipment Corporation's User Society (DECUS). Zu deren Angebot zählte eine Softwarebibliothek von Programmen, die Benutzer für eigene Zwecke geschrieben hatten. Man konnte sich aus einem gedruckten Katalog Anwendungen heraussuchen und bekam diese für den Preis der Erstellung einer Lochstreifen- oder Magnetbandkopie per Post zugeschickt. Die Kosten betrugen üblicherweise fünf bis fünfzehn Dollar, und da die Software copyrightfrei war, konnte man das Geld durch den Weiterverkauf von Kopien an Freunde und Bekannte wieder hereinbekommen.

Man konnte sich aus einem Katalog Anwendungen heraussuchen und bekam diese für den Preis der Erstellung einer Lochstreifen- oder Magnetbandkopie per Post zugeschickt.

Warum verschenkten 1969 Leute ihre Software? Im Wesentlichen, weil es schwer ist, Software zu verkaufen. Man muss für sie werben, Dokumentation erstellen, Support leisten, sie erweitern und zeigen, dass die Software „noch lebt". Darüber hinaus gab es 1969 in der IT keine Industriestandards. Jedes Stück Hardware besaß – wenn überhaupt – sein eigenes Betriebssystem. Da keine dominante Architektur existierte, war der Markt für Portierungen sehr klein. Außerdem waren die Autoren dieser Anwendungen keine professionellen Programmierer, sondern Ingenieure, Geschäftsleute, Anwälte, Lehrende oder Forscher. Sie verdienten ihr Geld mit anderen Dingen, brauchten aber Software als Unterstützung für ihren Job. Sie verschenkten ihre Software, damit andere davon profitieren und ihnen eventuell bei Verbesserungen helfen können. Als potenzieller Lohn winkte auf der DECUS vielleicht ein Freibier, ein kostenloses Essen oder mit viel Glück gar ein Jobangebot, aber Softwareverkauf hatten sie nicht im Sinn.

Zwei weitere Ereignisse trugen sich 1969 zu: In New Jersey entschlossen sich zwei AT&T-Forscher ein Betriebssystem zu schreiben, und im finnischen Helsinki kam ein Kind zur Welt. Dieser Artikel wird sich auf Ersteres konzentrieren.

Ken Thompson and Dennis Ritchie fingen mit der Entwicklung dessen an, was später als Unix bekannt werden sollte. Es begann als Forschungsprojekt und sie gingen nicht davon aus, dass es größere Auswirkungen auf die Computerindustrie haben würde. Sie wollten nur neue Wege für die Nützlichkeit von Computern suchen. Ken und Dennis verteilten ihre Software an viele Universitäten und verlangten – wenn überhaupt – nur einen kleinen Obolus zur Deckung der Kosten für Magnetbänder, Porto und Handbücher.

Und ein High-School-Student in New York City entschloss sich, mehr über diese Computer zu lernen.

Schon während seiner New Yorker High-School-Zeit hatte Richard M. Stallman (oder kurz: RMS) in IBMs Science Center und an der Rockefeller Universität gearbeitet. Später, im Jahr 1971, war Richard für Russ Noftsker am Labor für Künstliche Intelligenz des MIT (AI Lab) tätig – obwohl er nur ein Erstsemesterstudent in Harvard war. Wie Richard es ausdrückte: „Ich wurde Teil einer Software teilenden

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Community, die schon seit Jahren existierte. Die gemeinsame Nutzung von Software war nicht auf unsere besondere Community beschränkt; sie ist so alt wie Computer, genauso wie der Austausch von Kochrezepten so alt ist wie das Kochen. Aber wir praktizierten es mehr als die meisten.“

Das AI Lab verwendete ein Time-Sharing-Betriebssystem namens ITS (Incompatible Timesharing System), das Angestellte des Instituts für eine Digital PDP 10 entworfen und in Assembler geschrieben hatten. Als Mitglied der Community und als Angestellter des AI Lab war es Richards Job, dieses System zu verbessern.

Wir nannten unsere Programme nicht ‚Free Software‘, da der Begriff noch nicht geprägt war, aber das ist das, was es war.

„Wir nannten unsere Programme nicht ‚Free Software‘, da der Begriff noch nicht geprägt war, aber das ist das, was es war. Wann immer jemand von einer anderen Universität oder einer Firma ein Programm portieren und benutzen wollte, freute uns das und wir ließen sie gewähren. Wenn man ein unbekanntes interessantes Programm sah, konnte man immer den Sourcecode bekommen, sodass man ihn lesen, verändern oder sogar für eigene Anwendungen ausschlachten konnte.“

Nach einer Weile begannen jedoch Unternehmen Unix als potenziell gewinnbringendes Etwas zu betrachten. AT&T hatte die Software bis dato nie kommerziell freigegeben und fing an, sie zu lizenzieren. Darüber hinaus verlangte man von kommerziellen Firmen hohe Summen für die Weitergabe des Quellcodes. Unternehmen wie Sun starteten die Vermarktung günstigerer Unix-Binär-Distributionen etwa zur selben Zeit, als Microsoft und Apple anfingen, ihre Software nur in Binärform auszuliefern.

In der Usenix, die sich bekanntlich die Förderung fortschrittlicher Betriebssystemtechniken auf die Fahnen geschrieben hat, gab es eine leichte Änderung in den Konferenzpräsentationen. Während früher die Sprecher ihren Vortrag mit einer Adresse beendeten, von der man sich den Quellcode kopieren konnte, schlossen sie nun mit der Entschuldigung, dass ihr Arbeitgeber ihnen die Weitergabe des Quellcodes nicht gestattete. Die ersten Male quittierte das Publikum dies noch mit lautstarken Buh-Rufen, doch mit der Zeit wurden diese immer leiser und leiser. Die Zuhörer akzeptierten zunehmend die Tatsache vom Ende der freien Verteilung von Sourcecode – alle bis auf einen …

„Symbolics hat die Community des AI Lab zerstört,“ sagte RMS im Gespräch mit Peter Salus. „Die Leute kamen nicht mehr. 1980 verbrachte ich drei oder vier Monate in Stanford und als ich zurückkam [zum Tech Square], waren die Leute weg und das Labor quasi tot.“ Sam Williams erzählte [1], das Symbolics 14 Angestellte des AI Lab als Teilzeit-„Consultants“ eingestellt hatte. Richard war tatsächlich der „Letzte der Hacker“.

„Im Januar 1982 gaben sie [Symbolics] eine erste Version heraus,“ erzählte RMS weiter. „Sie teilten nicht, also implementierte ich einen ganz anderen Satz von Funktionen und schrieb etwa die Hälfte des Codes neu. Das war im Februar. An meinem Geburtstag [16.3.] brach der Krieg aus. Jeder am MIT entschied sich für die eine Seite: Nutze das Zeug von Symbolics, aber gib keinen Sourcecode weiter. Ich war sehr unglücklich. Die Community war zerstört worden. Nun begann sich das gesamte Verhalten der Leute zu ändern.“

Der erste Schritt zur Benutzung eines Computers bestand darin zu versprechen, seinem Nachbarn nicht zu helfen.

Was Richard Stallman wollte, war klar: Eine kooperative Community von Programmierern, die zunehmend bessere Software produzieren. Aber die Hersteller wollten keine Kooperation, jeder wollte ein partielles Monopol. Um die Software nutzen zu können, mussten Programmierer ein NDA (Non-Disclosure Agreement) unterschreiben. Richard sagte „Das bedeutete, der erste Schritt zur Benutzung eines Computers bestand darin zu versprechen, seinem Nachbarn nicht zu helfen. Eine zusammenarbeitende Gemeinschaft war verboten. Die von den Besitzern proprietärer Software aufgestellte Regel lautete: ‚Wenn du mit deinem Nachbarn teilst, bist du ein Softwarepirat.‘“

Richard hatte wiederholt gesagt, dass Software frei sein müsse. Aber 1982 und 1983 war er eine einzelne, einsame Stimme. Er kopierte die Arbeit der Symbolics-Programmierer, um zu verhindern, dass die Firma sich ein Monopol verschaffte. Er weigerte sich, NDAs zu unterschreiben und teilte seine Arbeit mit anderen, was er immer noch als den „Geist der wissenschaftlichen Offenheit und Zusammenarbeit“ ansah. Am 27. September 1983 kündigte RMS das GNU-Projekt an [a] und und gab im Januar 1984 seinen Job am MIT auf.

Er schrieb: „Ich begann mit der Arbeit am GNU Emacs im September 1984, Anfang 1985 begann er benutzbar zu werden. Dies ermöglichte mir, Unix-Systeme fürs Editieren einzusetzen. Ich hatte keine Lust, *vi* oder *ed* zu erlernen, da ich bis dahin meine Texte auf anderen Arten von Systemen erledigt hatte.“

Die gemeinsame Nutzung von Software ist so alt wie Computer – genauso wie der Austausch von Kochrezepten so alt ist wie das Kochen.

Zu dieser Zeit begann die 1982 gegründete Firma Sun Microsystems für ihr SunOS 4.1cBSD als Basis zu verwenden. In den folgenden rund sechs Jahren flossen alle BSD-Verbesserungen in die folgenden SunOS-Versionen ein. 1988 erschreckte AT&T die Unix-Community, indem man eine große Investition in Sun ankündigte. Offiziell hieß es, um die Unix-Bemühungen von AT&T und Berkeley zu vereinen, viele vermuteten jedoch weit dunklere Absichten.

Richard Stallmans erster Erfolg mit freier Software war der GNU C-Compiler (*gcc*). Zwar existierte schon eine Reihe von C-Compilern, (mindestens vier oder fünf von diesen stammten von P.J. Plaugers Firma Whitesmiths), aber die waren alle proprietär lizenziert. Stallmans Software war unbelastet und sie funktionierte gut. Heute steht GCC für GNU Compiler Collection, und umfasst Compiler für C, C++, Objective-C, Fortran, Java, Ada sowie eine große Zahl Bibliotheken. Das Zwei-CD-Set kostet nur 45 US-Dollar.

Dann verärgerte auch Sun seine Benutzer, indem es die Compiler nicht mehr im Bundle mit dem Betriebssystem sondern als eigenständige Produkte vermarktete. Während des Sun User Group Meeting in San Jose im Dezember 1990 spitzten sich die Dinge zu. Viele Sun-Nutzer fragten sich, warum sie einen C-Compiler von Sun kaufen sollten, wenn sie einen besseren und

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

billigeren bei der FSF bekämen. Als Ergebnis schnellten die CD-Verkäufe bei der FSF in die Höhe.

Stallman schrieb auch die GPL – die GNU Public License, heute GNU General Public License. Sie entstand aus dem Bedarf nach rechtlicher Dokumentation. Die Vorgeschichte der GPL begann damit, dass James Gosling, Jungakademiker an der CMU (Carnegie Mellon Universität), eine C-Version von Emacs schrieb. Gosmacs benutzte einen vereinfachten Lisp-Dialekt namens Mocklisp. Um seinen Emacs in Lisp zu schreiben bediente sich RMS bei Goslings Neuerungen. Andere CMU-Entwickler hatten Stallman erzählt, Gosling habe versichert, ihre Arbeit an Gosmacs und dem Lisp-Interpreter würde verfügbar bleiben. Aber Gosling stellte Gosmacs unter Copyright und verkaufte die Rechte an UniPress, die wiederum drohten, RMS zu verklagen.

Wieder einmal stand Stallman vor der Aufgabe, von vorn zu beginnen. Im Laufe des Reverse-Engineering von Goslings Interpreter sollte Stallman einen vollständigen Lisp-Interpreter schreiben, der Goslings Original nicht nur das Wasser reichen konnte. Dennoch: Die Idee, dass Entwickler Rechte an einer Software verkaufen – insbesondere der Gedanke, dass sie überhaupt Rechte an einer Software besitzen, die sie verkaufen können, wurmte Stallman gehörig.

Insbesondere der Gedanke, dass Entwickler überhaupt Rechte an einer Software besitzen, die sie verkaufen können, wurmte Stallman gehörig.

1985 gab RMS zwar den GNU Emacs frei, aber er musste realisieren, wie wichtig es für GNU-Software sei, auf ein rechtliches Fundament bauen zu können. Als direktes Ergebnis entstand die erste Version der GPL. Richard hatte erkannt, dass man den Benutzern ein uneingeschränktes Recht einräumen müsse. Zwar hatte er mit dem Bostoner Anwalt Mark Fischer, spezialisiert auf geistiges Eigentum, sowie einem weiteren Anwalt, Jerry Cohen, gesprochen, aber dennoch schrieb er seine eigene Lizenz. Nur wenige Jahre später erschien die GPL Version 2.

Das war 1991. Bis 1991 gab es viele Leute, die GNU-Software auf unterschiedlichen Plattformen einsetzten. Richard war so weitsichtig gewesen (vielleicht hatte er auch nur Glück), eine Software zu entwerfen, die sich auf viele Betriebssysteme und Hardwarekombinationen portieren ließ. Er kümmerte sich zuerst um „Upper-Level“-Anwendungen, statt sich an einem Kernel zu versuchen. GNU-Software kam zum Einsatz, um Unterschiede zwischen den Hard- und Softwarekombinationen unterschiedlicher Hersteller zu überwinden. Der Emacs verhielt sich auf allen Plattformen gleich. Boeing benutzte die GNU-Compiler, weil Syntax und Semantik auf den unterschiedlichen Systemen gleich waren, was zu weniger Ausnahme-Routinen im Quellcode eines Projekts führte. Kunden von Firmen wie DEC begannen zu fordern, dass GNU-Code auch auf die proprietärsten Systeme portiert und mit ausgeliefert werden sollte. Weigerten sich die Firmen, verloren sie Kunden.

Maddog, damals Manager bei DEC, erinnert sich an eine solche Anforderung, GNU-Code unter dem Namen „Goodstuff“ zu vertreiben. Es handelte sich um eine Programmsammlung übersetzt für Digital Unix auf dem hauseigenen Alpha-Prozessor. Da diese offiziell als „unsupported“ galt, fragte sich fast das gesamte DEC-Softwareproduktmanagement ungläubig, warum Kunden gerade diese Software haben wollten. Und doch verteilte DEC Tausende dieser CDs an die Kunden und ersparte ihnen die Mühe, die Software selbst zu bauen. Später, als das Alpha-Linux-Projekt schon lief, war die Entwicklungsabteilung bei DEC überrascht, dass sich der Großteil des Upper-Level-Codes sich so leicht auf ein 64-Bit-System portieren ließ. Maddog wusste, dass der Code bereits auf Digitals Unix auf Alpha-Systemen portiert worden war, sodass – wenn überhaupt – nur wenige Probleme zu erwarten waren.

Allerdings war es nicht immer einfach, mit Richards Idealen umzugehen. Maddog erinnert sich an seine Bemühungen, der FSF einen VAX/Ultrix-Rechner zur Verfügung zu stellen, damit sie ihre GNU-Software auf das System portieren konnte. Erst nach vielen vergeblichen Anläufen ließ sich Richard dazu bewegen, ein Digital-Standardformular mit dem Titel „Leihgabe von Produkten“ zu unterschreiben. Der Grund: Ihn störte die Passage, die einen Schutz des Betriebssystems vor Kopien forderte. Während Richard DEC versicherte, er würde das Betriebssystem nicht kopieren, weil er gar nicht den Wunsch dazu verspüre, würde er doch niemanden abhalten es zu tun, weil es seiner Überzeugung widerspreche. Ein Federstrich eliminierte den betreffenden Satz, ein paar Initialen und alles war in Butter.

In Bezug auf freie Software existierten auch andere Projekte, die sich – natürlich – in den Freiheitsgraden der verwendeten Lizenzen unterschieden. Die Berkeley Software Distributions, das MIT-Projekt Athena (von dem Kerberos und das X Window System heute noch als Erbe erhalten sind), Sendmail, Ingres/Postgres und andere. Aber das GNU-Projekt überflügelte sie alle mit seinem einzigartigen Ziel, eine komplette Betriebssystemumgebung zu schaffen, deren Quellcode verfügbar ist und die den vier in der GPL erklärten Freiheiten genügt.

Eine kooperative Community von Programmierern produziert zunehmend bessere Software.

Um 1991 herum existierte in der einen oder anderen Form der Code für viele Komponenten eines Betriebssystems. Der einzig fehlende Hauptteil war der Kernel. Obwohl unter dem Namen „The Hurd“ auch ein GNU-Kernel-Projekt geplant war, sorgten diverse Richtungswechsel und andere Verzögerungen dafür, dass der Linux-Kernel viele Teile des GNU-User-Level-Codes nutzen konnte.

Jetzt feiert das GNU-Projekt seinen fünfundzwanzigsten Geburtstag. Viele Leute haben Richard Stallman für sein taktisches Vorgehen kritisiert. Aber in der Realität gibt es nur wenige Menschen, die ihre Philosophie und Ziele klar definieren und über ein Vierteljahrhundert konsequent in die Tat umsetzen. Sicherlich hätten viele Informatikstudenten weniger Erfahrungen gesammelt, hätten sie nicht den Zugriff auf den Quellcode von ausgezeichneter Software gehabt – entwickelt unter der Philosophie von Richard Stallmans Free Software Foundation und dem GNU-Projekt. (avr)

Literatur

[1] Sam Williams; Free as in Freedom; Richard Stallman’s Crusade for free Software; ISBN 978-0-596-00287-9; O’Reilly 2002

[2] Richard M. Stallman, Ankündigung des GNU-Projekts; groups.google.com/group/net.unix-wizards/msg/4dadd63a976019d7?output=gplain

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Ad-hoc-Software aus der Fachabteilung

Zusammengerührt

Volker Hoyer

Eine neue Generation von Webanwendungen verändert die Softwareentwicklung grundlegend. Mit Enterprise Mashups soll der Benutzer auf Basis verteilter Webservices sogenannte situationsbezogene Anwendungen innerhalb von Minuten selbst erstellen.

Cloud Computing, On Demand und Software as a Service (SaaS) wollen alle das Eine: weg von lokalen Anwendungen hin zu Diensten, die irgendwo im Internet liegen können. Unternehmen hoffen, dass sich dadurch der Aufwand für Inbetriebnahme und Pflege komplexer Software deutlich reduziert. Diese Arbeiten, ebenso wie das Lösen von Interoperabilitätsfragen, übernehmen dabei externe Dienstleister. Bislang beschränkt sich das Auslagern von Services ins Web jedoch auf komplette Programmpakete. Produkte wie Salesforce, Microsofts Dynamics oder SAPs Business By Design bestimmen heute den SaaS-Markt.

Enterprise Mashups gehen einen Schritt weiter [1], [2]. Die Idee dabei: Der Anwender kombiniert kleine, fertig zurechtgeschneiderte Dienste miteinander und soll so situationsbezogene Aufgaben selbst und vor allem schnell lösen. Beispielsweise könnte er einfache RSS oder Atom Feeds mit Landkarten oder auch leistungsstarken Webservices verknüpfen, etwa um sich aktuelle Verkaufsergebnisse in bestimmten Regionen anzeigen zu lassen.

Im Gegensatz zu serviceorientierten Architekturen (SOA), hinter denen aufwendige Standards (WSDL, UDDI, SOAP) stehen, richten sich Enterprise Mashups explizit an den Endanwender, der in der Regel nicht über Programmierkenntnisse verfügt. Schon das Auslagern der kleinen alltäglichen IT-affinen Verrichtungen würde die ansonsten zuständigen technischen Abteilungen merklich entlasten [3]. Die von den Fachabteilungen gestrickten Anwendungen sollen nicht perfekt sein, lediglich „gut genug“, um die jeweilige Ad-hoc-Anforderung zu erfüllen. Traditionelle Versionen der Programme gibt es in diesem Szenario nicht mehr; es herrscht der permanente Beta-Zustand. Da die ganze Sache noch am Anfang steht, bleiben eine Menge Fragen offen, etwa die nach einem zuverlässigen Zugriffs- und Berechtigungskonzept, wenn es beispielsweise um sensible Unternehmensdaten aus ERP-Systemen geht. Hier ist die IT-Abteilung nach wie vor gefordert. Beispielsweise könnte sie die Mashup-Erstellung in eine Portalumgebung einbinden, die üblicherweise Rollenkonzepte vorsieht.

Eine bedeutende Rolle spielt in diesem Umfeld der Community-Gedanke. Benutzer beschreiben, bewerten und kommentieren die verschiedenen Komponenten (Ressourcen, Widgets und Mashups) und tauschen auf diese Weise Erfahrungen und bewährte Verfahren (Best Practises) aus. Jedes einmal angelegte Mashup soll sich so mit kleinen Anpassungen in ähnlichen Kontexten wieder verwenden lassen.

Etliche Softwarehersteller haben das Potenzial der neuen Technik erkannt und bieten Werkzeuge für diesen schnell wachsenden Markt an. Das Marktforschungsunternehmen Forrester erwartet bis zum Jahre 2013 ein Marktvolumen von 700 Mio. Dollar. Da sich in Bezug

iX-TRACT

- Enterprise Mashups sind kleine Anwendungen des täglichen Bedarfs, die sich der Benutzer selbst aus verschiedenen Webservices zusammenstellt.
- Mit öffentlichen Ressourcen wie Foto- und Videoplattformen, sozialen Netzwerken und Kartendiensten kommen die vorgestellten Tools gut klar. Was noch allen fehlt, ist die professionelle Einbindung in Unternehmenssoftware.
- Sobald genug fachliche Webservices zur Verfügung stehen, könnten Enterprise Mashups die traditionelle Softwareentwicklung um eine interessante Facette erweitern.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

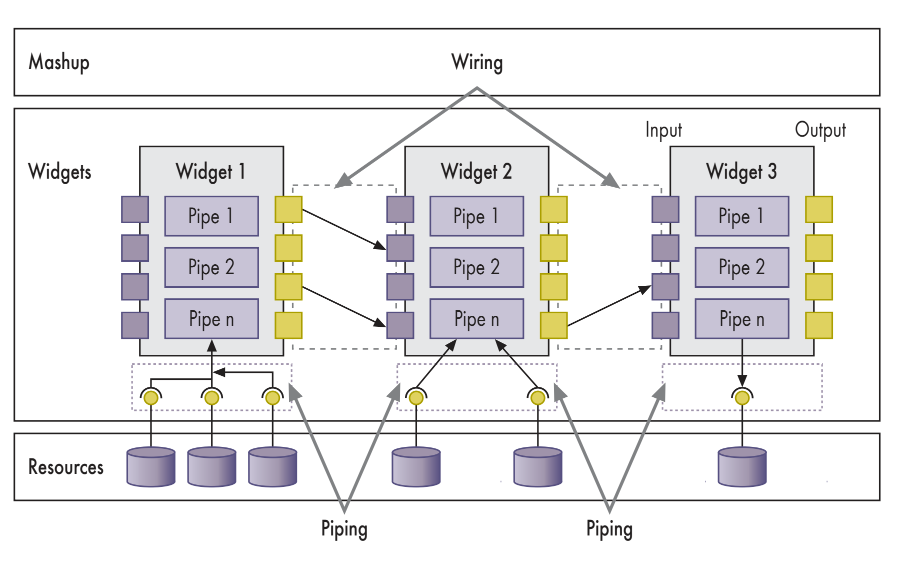
auf Enterprise Mashups bislang keine saubere Terminologie durchgesetzt hat, sind die Designprinzipien nur an ihren Kerneigenschaften zu erläutern. Auf der unteren Ebene der zugrunde liegenden Schichtenarchitektur liegen Inhalte, Daten und Funktionen. Standardisierte Schnittstellen (WSDL, RSS, Atom, JSON, CSV et cetera) abstrahieren von diesen Ressourcen und trennen Implementierung und Spezifikation. Sie erlauben somit die lose Kopplung der verschiedenen Ressourcen, was auch die zentrale Forderung von SOA erfüllt (Abbildung 1).

Auf der darüberliegenden Ebene kapseln Widgets den Zugriff auf die technische Basis und geben ihr eine Oberfläche [4]. Diese kleinen Dienstprogramme kann der Benutzer beliebig verknüpfen und konfigurieren. Als Ergebnis seiner Komposition erhält er ein Mashup. Ähnlich wie beim Unix-Pipeline-Konzept schaltet der Arrangeur die verteilten Ressourcen hintereinander (Piping) und verbindet sie mittels Operatoren (beispielsweise Aggregation, Filter, Sortierung) über ihre Input und Output Ports (Wiring). Im Folgenden wird eine Auswahl von Werkzeugen mit unterschiedlichen Schwerpunkten vorgestellt (siehe Tabelle „Mashup-Werkzeuge für den Unternehmenseinsatz“). Eine ausführliche Liste von Tools zum Thema liefert der *iX*-Link am Ende des Textes.

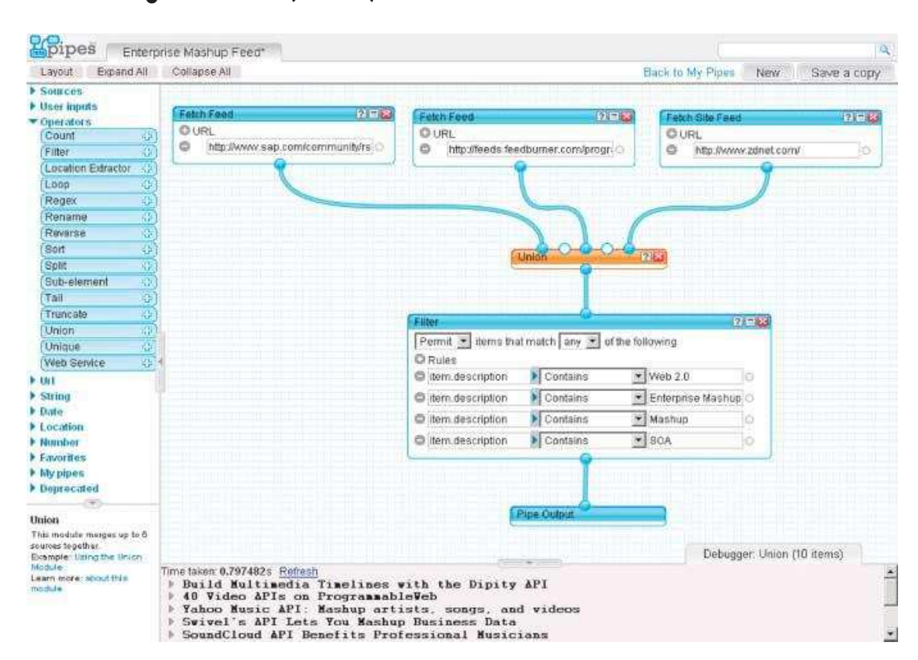


Yahoo Pipes

Als Mashup-Pionier gilt Yahoo Pipes. Mit dem Produkt lassen sich Informationen aus beliebigen Datenquellen mittels verschiedener Operatoren transformieren und veröffentlichen. Pipes verlangt zwar keine Programmierkenntnisse, allerdings sollte man ein grundlegendes Verständnis über Datenformate und logische Operatoren mitbringen.



Per Piping und Wiring führt der Anwender Ressourcen und Widgets zu einer Anwendung zusammen (Abb. 1).

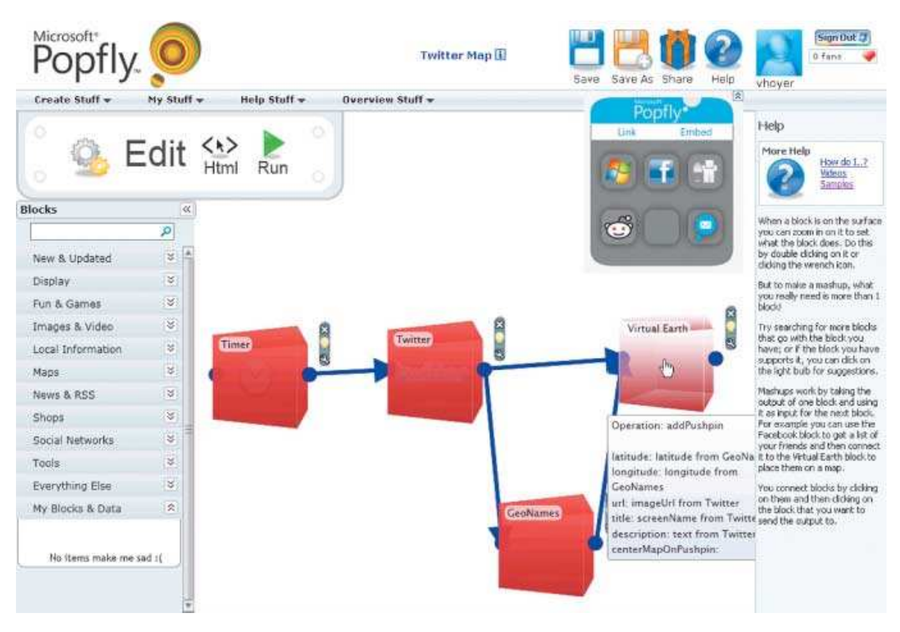


Ohne Programmierung zum Mashup: Yahoo Pipes (Abb. 2)

Die Arbeitsumgebung der Webanwendung teilt sich in drei Bereiche (Abbildung 2). Links liegen die verschiedenen Funktionsmodule, die sich per Drag & Drop in den Modellierungsbereich ziehen lassen. Der Debugger



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Microsoft geht das Thema Enterprise Mashups spielerisch an (Abb. 3).

(unten) bietet die Möglichkeit Zwischenergebnisse zu prüfen. Vor allem bei komplexen Operationen leistet die Vorschau gute Dienste. Die Module werden mittels sogenannter Pipes verknüpft und definieren somit den Datenfluss. Ressourcen können RSS oder Atom Feeds sein, aber auch Textdateien im CSV-Format (Comma Separated Values).

Pipes beschränkt sich auf wenige öffentliche Informationsquellen. Es stehen lediglich Google Base (Artikelbeschreibungen), Flickr (Fotoplattform) und Yahoo Search als Ressourcen zur Verfügung. Der Anwender kann verschiedene Feeds sortieren, filtern oder zusammenführen. Es ist noch nicht möglich, Unternehmensapplikationen einzubinden. Hilfreiche Dienste leistet ein umfangreiches Verzeichnis mit mehr als 1000 vorgefertigten Pipes, die der Benutzer für die jeweilige Aufgabe anpassen kann. Ferner lassen sich die Ressourcen als Widgets (bei Yahoo Badges genannt) in Mashup-Plattformen wie iGoogle, Netvibes, My Yahoo, Netvibes oder My-AOL einbinden. Präferierte Darstellungselemente sind einfache Tabellen (RSS Feeds), Bilder oder Landkarten.

Microsoft Popfly

Mit Microsofts Popfly erstellt der Anwender Webanwendungen, Mashups und Spiele. Über die Oberfläche, die auf Silverlight aufbaut, positioniert er eine Reihe von Objekten, sogenannte Blocks. Letztere bilden Ressourcen sowie Operatoren ähnlich denen von Yahoo Pipes ab. Das funktioniert ohne Programmierkenntnisse. Wer welche hat, kann zusätzlich neue Blocks in Javascript erstellen. Als Entwicklungsumgebung fungiert ein einfacher Editor. Interessantere Optionen und mehr Komfort bietet jedoch die Integration des Werkzeugs in Visual Studio. Popfly richtet sich eindeutig an den privaten Konsumenten. Neben Fotos (Flickr, Google Picasa, Yahoo Image) und Videos (Yahoo Video), Karten (Virtual Earth, Yahoo Traffic, Yahoo Geo Coding) und Shops (MSN Shopping) bietet die Einbindung von sozialen Netzwerken (Facebook, Live Space, Technorati, Twitter, Xbox Live) vielfältige Möglichkeiten für die Konstruktion von Mashups.

Den Datenfluss steuert und konfiguriert der Anwender anders als bei Yahoo

Mashup-Werkzeuge für den Unternehmenseinsatz

Produkt	Yahoo Pipes	Microsoft Popfly	SAP Research Rooftop	Serena Mashup Suite	IBM Mashup Center
Website	pipes.yahoo.com/pipes/	www.popfly.com	www.sap.com/research	www.serena.com/mashups/	alphaworks.ibm.com/tech/ibmmsk
Lizenz	frei verfügbar	frei verfügbar	kein Produkt (soll sich ändern)	30 Tage Testversion verfügbar	Hosted-Version frei verfügbar
Marktbereich	Consumer/Enterprise	Consumer	Enterprise	Enterprise	Enterprise
Systemvoraussetzung	Firefox, IE	Plug-in Silverlight, Firefox, IE	IE	IE	Firefox, IE 7, Safari
Komposition					
Prozessunterstützung	nein	nein	nein	ja	nein
visuelles Wiring	nein	nein	ja	nein	ja (Lotus Mashups)
visuelles Piping	ja	ja	nein	nein	ja (Infosphere Mashup Hub)
Mashup-Katalog					
Ressourcen	Feeds	Flickr, Google Picasa, Yahoo-Dienste, Virtual Earth, MSN Shopping, Facebook etc.	SAP Enterprise Services, Youtube, Virtual Earth, Flickr, Feeds	keine speziellen	Open Street Map, Google Gadgets, Youtube, Virtual Earth, Feeds
Darstellung von Widgets	einfache Tabellen, Bilder und und Karten	Tabelle, Bilder, Karten, Balkendiagramm, Kreisdiagramm	Tabelle, Bilder, Karten	Oberflächen für Prozessschritte via Form Designer	Tabelle, Bilder, Karten, Diagramme, individuell via Javascript
Ressourcentypen	RSS, Atom, JSON, RDF, CSV, HTML, XML, KML (Flickr, Google Base, Yahoo Search)	RSS, XML, CSV	Webservices, REST, RSS Feeds, XML	Webservices	Webservices, Feeds, CSV, SAP, SQL, Domino Server, LDAP, IMS Transaction etc.
Zusammenarbeit					
Tagging	ja	Widgets	nein	ja	ja
Empfehlungen/Bewertungen	ja	nein	nein	ja	ja
Erfahrungsaustausch	indirekt über Pipes	nein	nein	ja	ja
Beispiele	über 1000 Yahoo Pipes	kaum vorhanden	über 500 Mashups	über 30 (Sales, IT, HR etc.)	40 Beispiel-Mashups
Sonstiges					
Debugger	ja	ja	nein	nein	nein
Dokumentation	ausreichend, Wiki	gering	nein	gering	umfangreich, mehrsprachig
Besonderheiten	Piping-Pionier	Integration in Visual Studio	Integration von SAP Enterprise Services	Office-artiger Stil	Integration von Programmableweb.com

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Pipes mit dreidimensionalen Elementen, Popfly nähert sich der Mashup-Erstellung eher spielerisch (Abbildung 3). Leider erfordert es eine gewisse Einarbeitungszeit, die rotierenden roten Blöcke mittels der blauen Konnektoren zu verknüpfen. Jeder Block zeigt sinnvolle Verbindungen zu anderen Blocks mit einer gelbe Glühbirne an. Popfly bietet eindrucksvolle Anzeigeoptionen für die Kombination der Ressourcen an. Nicht nur Karten und einfache Tabellen stehen zur Verfügung, sondern auch Alben, interaktive Bilderkarussells, Slideshows, Kreis- und Balkendiagramme.

Hat der Benutzer alle Blocks miteinander verbunden und ein Ausgabeformat gewählt, kann er sich das Ergebnis in einer Vorschau anzeigen lassen. Ein einfacher Debugger hilft ihm dabei, die internen Aufrufe nachzuvollziehen und gegebenenfalls Probleme zu erkennen. Die Widgets lassen sich via Menüpunkt „Share“ als Vista Gadget, Windows Live Gadget (in der Windows Live Gallery) oder bei Facebook veröffentlichen.



SAP Research Rooftop

Von SAP gibt es bislang lediglich einen Prototypen zum Erstellen von Enterprise Mashups. Das Tool mit dem Namen Rooftop ermöglicht es, SAPs Enterprise Services mit externen Webservices zu kombinieren (Abbildung 4). Rooftop lässt sich innerhalb des hauseigenen Portals, als separate Anwendung und darüber hinaus auf Mobiltelefonen mit Symbian-Betriebssystem ausführen. In einem aktuellen Projekt konzipierten die Entwickler beispielsweise eine Portalanwendung für die Neuverhandlung von Einkaufskontakten in der ERP-Plattform Business By Design. SAP setzt eine Reihe von mit Rooftop angelegter Mashups produktiv ein, etwa das SAPcon Widget, das Manager weltweit über den Gesamtstatus der IT-Landschaft informiert. Der Rooftop-Prototyp findet gerade Eingang in das SaaS-Produkt Business By Design.



Noch im Experimentierstadium: Rooftop von der SAP (Abb. 4)



Serena Mashup Suite

Einen anderen Schwerpunkt als die anderen hier aufgeführten Werkzeuge setzt die Mashup Suite von Serena. Sie vereint den Mashup-Gedanken mit dem prozessorientierten Ansatz. Das Produkt besteht aus einem Composer, einem Server sowie der Download-Plattform Marketplace Exchange. Vorgefertigte Mashups für verschiedene Unternehmensbereiche (Verkauf, IT, Personal, Finanzen, Kundendienst) kann sich der Interessierte über Marketplace Exchange herunterladen. Empfehlungen und Bewertungen lassen sich hier hinterlegen.

Analog zur klassischen Softwareentwicklung stellt der Mitarbeiter aus der Fachabteilung seinen individuellen Prozess im Composer zusammen. Dessen Oberfläche orientiert sich an Microsofts Office-Produkten. Da die jeder kennt, fällt das Einarbeiten in die Prozessmodellierung leicht. Letztere erfolgt mit einfachen Aktivitäten (beispielsweise Webservices), die miteinander verbunden werden. Jedem Prozessschritt kann der Benutzer eine Rolle zuweisen. Ein Form-Designer hilft ihm dabei, die Oberflächen für die Prozessschritte aus einer Palette grafischer Elemente zu erstellen (Abbildung 5). Der Mashup-Server, der verschiedene Monitoring-Administrationsfunktionen bietet, führt schließlich die Prozesse aus.



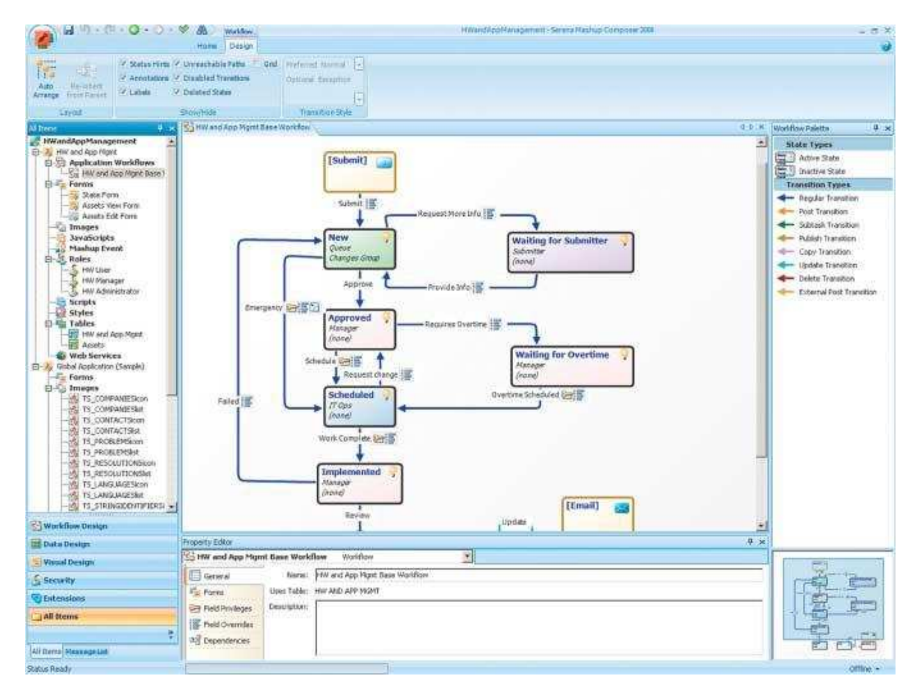
IBM Mashup Center

Eine Vorreiterrolle in Sachen Mashups für Unternehmensumgebungen spielt IBM. Ab dem vierten Quartal dieses Jahres will man ein entsprechendes Produkt anbieten. Es besteht aus den beiden Komponenten Lotus Mashup und Infosphere Mashup Hub.

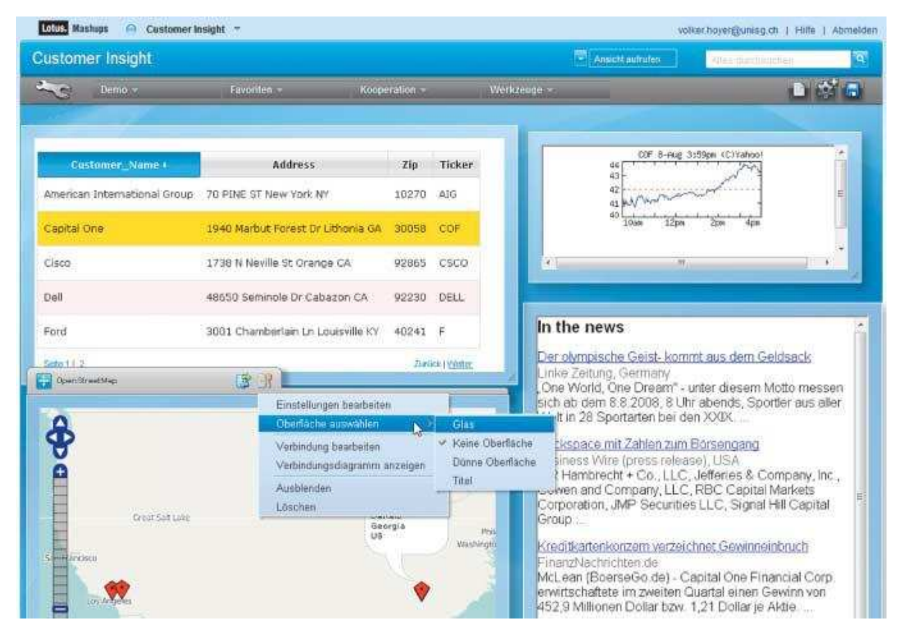
Mashup Hub beinhaltet einen Katalog für alle drei technischen Ebenen (Ressourcen, Widgets und Mashups). Hier liegen auch die Community-Komponenten wie Tags und Bewertungen.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Serena kombiniert Unternehmensprozesse mit Mashups (Abb. 5).



IBMs Mashup Center bietet zahlreiche Unternehmensressourcen an (Abb. 6).

Der Benutzer kann sogenannte Feed-Mashups erstellen, die dafür zuständige Umgebung enthält eine Reihe von Operatoren und Funktionen, mit denen er Daten importiert, sie bearbeitet und das Ergebnis als neuen Feed veröffentlicht. Bedienung und Steuerung sind vergleichbar mit der von Yahoo Pipes.

Neben RSS und Atom Feeds unterstützt Mashup Hub eine Reihe weiterer Ressourcentypen. Dazu gehören DB2 XML Columns, Domino Server, IBMs Information Server, IMS-Transaktionen, LDAP, SQL-Datenbanken, SAPs Applikationsfunktionen, Tivoli Directory Integrator, Webservices, Excel, CSV, Access und XML. Mittels Mashup Hub erstellt der Benutzer auch die Widgets, die er anschließend an Lotus Mashups weiterreicht. Zusätzlich bietet IBM dem Programmierer mit der Lotus Widget Factory eine Eclipse-basierte IDE.

Lotus Mashups ist die Umgebung für die Fachabteilung, die mit diesem Werkzeug die Widgets zu Mashups kombiniert (Abbildung 6). Standard-Widgets (Open Street Map, Google Gadgets, Youtube, HTML-Seiten, Bilder, Slideshows, Balken- und Kreisdiagramme et cetera) kann der Benutzer zu seinem Mashup hinzufügen. Die Widgets lassen sich frei im Mashup positionieren und konfigurieren. Für die optische Aufbereitung stehen verschiedene Oberflächen (Skins) zur Verfügung. Die Verbindungen zwischen den Widgets (Wiring) werden über einen einfachen Dialog angelegt. Ein Verbindungsdiagramm zeigt alle Konfigurationen übersichtlich an. Insgesamt hinterlässt IBMs Mashup Center einen ausgereiften und aufgeräumten Eindruck. Beide Kompositionsebenen, Piping und Wiring, deckt es adäquat ab. Leider existieren bislang noch nicht viele fachliche Widgets.

Fazit

Man kann davon ausgehen, dass Mashups für den schnellen Aufbau von Ad-hoc-Applikationen an Bedeutung gewinnen werden. Die vorgestellten Werkzeuge können zwar mit öffentlichen Ressourcen wie Foto- und Videoplattformen, Kartendiensten, sozialen Netzwerken et cetera umgehen, die direkte Integration in einschlägige Unternehmenssoftware bietet jedoch noch keines. IBMs Mashup Center zeigt, wie es gehen könnte. Das volle Potenzial von Enterprise Mashups wird sich erst dann erschließen, wenn Hersteller und Community genug vorgefertigte Widgets mit Unternehmensfunktionen zur Verfügung stellen. (jd)

VOLKER HOYER

ist Doktorand am Institut für Medien- und Kommunikationsmanagement an der Universität St. Gallen und bei SAP Research CEC St. Gallen, Schweiz.

Literatur

[1] Ramon Wartalla; Webprogrammierung; Weltbaukasten; Mashup: eine Revolution in Zeiten des Web 2.0; *iX* 7/2006, S. 54

[2] Volker Hoyer, Katarina Stanoevska-Slabeva, Till Janner, Christoph Schroth; Enterprise Mashups: Design Principles towards the Long Tail of User Needs; In Proceedings of the IEEE International Conference on Service Computing (SCC 2008)

[3] Volker Hoyer, Katarina Stanoevska-Slabeva; Enterprise Mashups – Neue Herausforderungen für das Projektmanagement; HMD – Praxis der Wirtschaftsinformatik, Heft 260



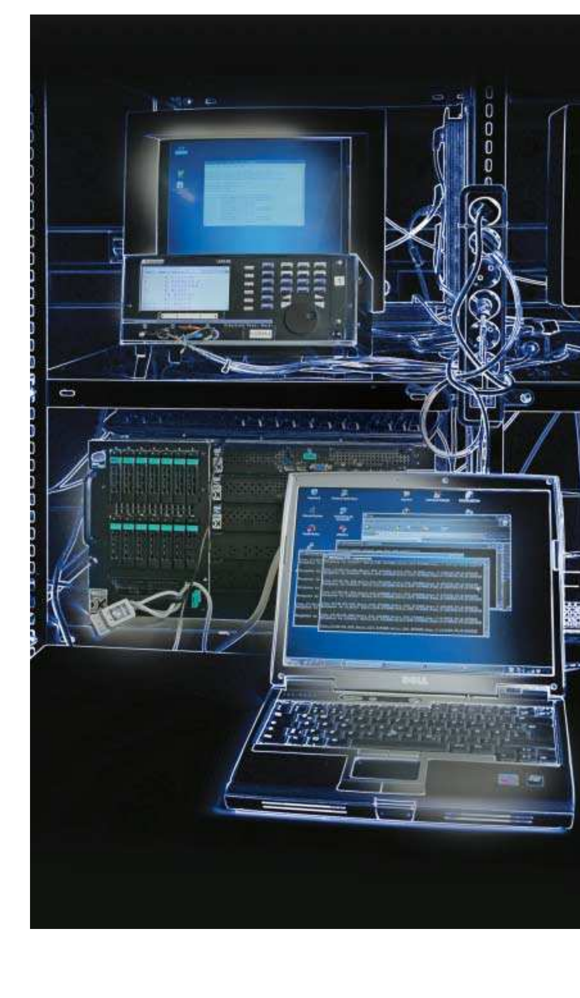


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Energieeffizienz messen mit SPECpower

Power-Spezial

Ralph Hülsenbusch



Was Computer beim Rechnen an Strom verbrauchen, gewinnt angesichts der steigenden Energiepreise mehr und mehr an Bedeutung. Deshalb entstand bei der SPEC ein spezieller Benchmark, dem sich im *iX*-Labor einige Systeme stellen mussten.

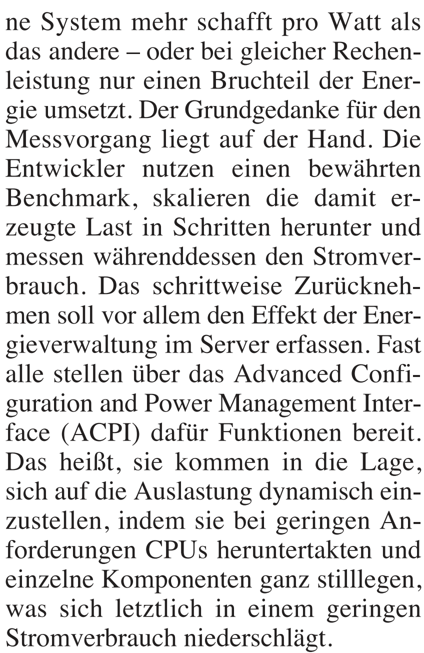
Wer misst, misst Mist, titelte *iX*-Autor Hubert Sieverding [1] vor fast 15 Jahren, als er sich grundsätzlich mit dem Thema synthetische Benchmarks auseinandersetzte. Damals ging es um die Leistungsfähigkeit von Systemen, vor allem um symmetrische Multiprozessoren. Heutzutage zählen Benchmark-Ergebnisse immer noch zu den vor allem in Werbeaussagen beliebten Zahlen, obwohl sie in vielen Fällen gar nicht die passenden Entscheidungskriterien liefern. Die Leistung und das Volumen der Ressourcen sind seit der Einführung der Multi-Core-Prozessoren sprunghaft angestiegen, die Chips geschrumpft.

Unter dem Strich schlagen die Unterschiede in den Performancedaten für den alltäglichen Einsatz eines Servers kaum zu Buche, dafür aber der Energiehunger. Denn was die Systeme konsumieren, müssen Kühlsysteme wieder fortschaffen. Das stößt an Grenzen: Racks lassen sich mit den kompakten 1U-Rechnern nicht mehr komplett bestücken, weil es sonst zu einem Wärmestau käme. Die Ausnutzung der Räume nimmt ab, da nicht die Raumgröße, sondern die Leistung der Klimaanlagen die Zahl der Server begrenzt, und in einigen Fällen können die Stromlieferanten den Bedarf von Rechenzentren nicht mehr abdecken.

Wachsende Akzeptanz

Deshalb stellt sich die Frage, wie viel Performance ein System pro Energieeinheit erreichen kann. Die Mitglieder der Standard Performance Evaluation Corporation (SPEC), einer gemeinnützigen Herstellervereinigung, haben 2007 den Benchmark SPECpower_ssj2008 unter Zuhilfenahme von Server Side Java entwickelt. Als Ergebnis gibt der Test Operationen pro Watt (ops/watt) aus. Ende 2007 mit der offiziellen Freigabe des Tests haben die ersten fünf Hersteller 12 Resultate auf der SPEC-Site veröffentlicht. Die Werte schwanken zwischen 87,5 und 698. Inzwischen – Stand August 2008 – sind es zehn Produzenten mit 48 Systemen, und die Spanne hat sich auf 1124 ausgedehnt; im Vergleich zu anderen Benchmarks bei der SPEC eine schwache Resonanz. Beim zeitraubenden CPU2006 waren es in den beiden ersten Monaten zehn Firmen mit 28 Rechnern.

Ohne Kenntnisse des Hintergrundes verraten die *ops/watt* nur, dass das eine System mehr schafft pro Watt als das andere – oder bei gleicher Rechenleistung nur einen Bruchteil der Energie umsetzt. Der Grundgedanke für den Messvorgang liegt auf der Hand. Die Entwickler nutzen einen bewährten Benchmark, skalieren die damit erzeugte Last in Schritten herunter und messen währenddessen den Stromverbrauch. Das schrittweise Zurücknehmen soll vor allem den Effekt der Energieverwaltung im Server erfassen. Fast alle stellen über das Advanced Configuration and Power Management Interface (ACPI) dafür Funktionen bereit. Das heißt, sie kommen in die Lage, sich auf die Auslastung dynamisch einzustellen, indem sie bei geringen Anforderungen CPUs heruntertakten und einzelne Komponenten ganz stilllegen, was sich letztlich in einem geringen Stromverbrauch niederschlägt.



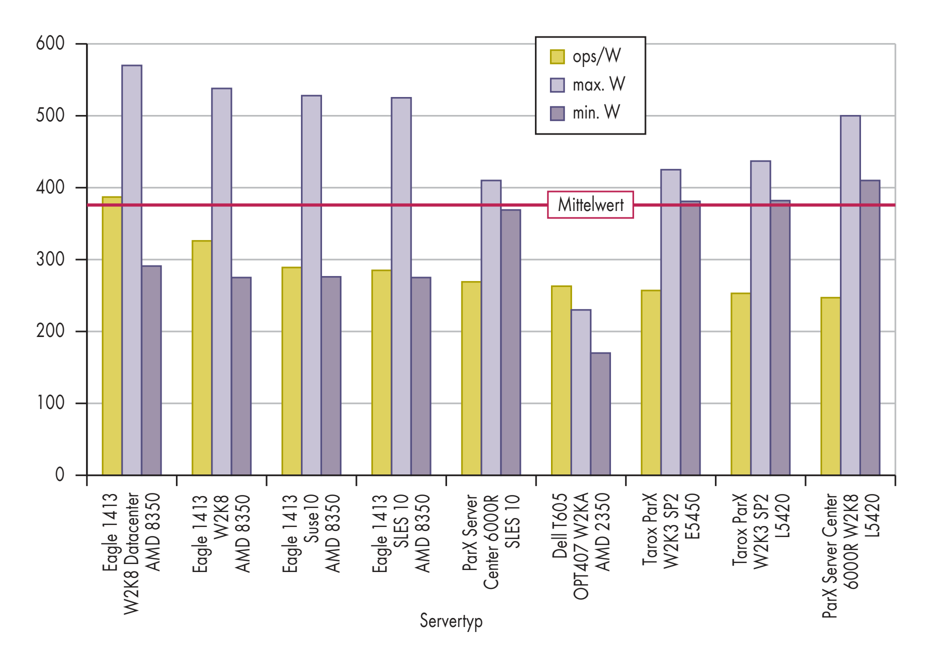
Als Last wählten die Entwickler eine Ableitung des SPEC JBB2005 [4], des Java Business Benchmark, der in der virtuellen Java-Maschine die Geschäftsprozesse mehrerer Warenhäuser nachbildet: die Server Side Java Business Application Simulation. Über eine festgelegte Laufzeit ermittelt der Test, wie viele Operation pro Sekunde im SSJ der Rechner schafft.

Ein zweiter Rechner fungiert als Kontrollinstanz. Er überwacht die Raumtemperatur vor der Luftansaugöffnung des zu untersuchenden Servers – des System under Test (SUT) –, die Luftfeuchte und die vorgegebene Netzspannung. Temperaturen unter 20° C und Über- oder Unterschreitung der Netzspannung um mehr als 5 % sowie der Netzfrequenz um mehr als 1 % ahndet Power_ssj2008 mit einem ungültigen Resultat.

Zusammenspiel der Komponenten

Für die extern angeschlossenen Messgeräte gibt es bei der SPEC strenge Vorschriften, was die Messtoleranzen und Messbereiche angeht. Außerdem müssen sie im selben Jahr, in dem der Messvorgang stattfindet, kalibriert worden sein. Darüber hinaus gelten die von der Open Systems Group (OSG), einer Untergruppe der SPEC, vorgegebenen Regeln der Fair Use Policy. All das hat den Sinn, zu verhindern, dass Hersteller ihre Computer schönrechnen, in

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Grundrauschen: Server im Alltagsbetrieb verbrauchen ohne Last 300 W und mehr. Da schlagen die Energiesparmaßnahmen der Prozessoren kaum zu Buche (Abb. 1, sortiert nach ops/W).

dem sie zum Beispiel den Server im Kühlhaus laufen lassen.

Wenn das Testfeld aufgebaut und verkabelt ist, muss der Prüfer die Java-Maschinen einrichten. Danach kann er auf beiden Rechnern die Testsuite per *setup* installieren. Zuerst startet er nach dem Einschalten der Messgeräte auf dem Steuerrechner *runpower* und *runtemp* als *.bat* oder *.sh* – je nach Betriebssystem. Im *iX*-Labor war es ein Laptop unter Windows XP, den Kollegen von der c't eingerichtet hatten [5]. Beide Jobs verharren in Warteposition, bis der Tester das eigentliche Steuerprogramm *runCCS* startet. Das wartet nun darauf, dass er auf dem Server (SUT) den Benchmark mit *runssj* aktiviert, der daraufhin ein Signal über einen Port an den Kontrollrechner sendet, woraufhin das gesamte Gespann mit der Messprozedur beginnt.

Umgebungsfaktoren

In einem der Fenster kann der Tester Temperatur und Luftfeuchtigkeit sowie in einem anderen die elektrische Kenndaten mitlesen. Im dritten, dem von *runCCS*, erscheinen Nachrichten über den Fortschritt des Messlaufes.

Zuerst führt der Benchmark drei Kalibrierungen unter Volllast durch, die das Maß für alle weiteren Durchgänge liefern. Bei einer Abweichung von mehr als 2 % (+2 % und -2,5 % bei 100 % und 80 % Last) bricht Power_ssj2008 ab. Ebenso empfindlich reagieren *runCCS* und *runssj* aufeinander: Stirbt einer der beiden, terminiert das den anderen. Dagegen sind die Messroutinen toleranter; versagen sie, läuft der Benchmark zwar weiter, aber das Resultat ist ungültig. Das liefert zwar einen Wert für *ssj_ops*, hat aber zur Folge, dass man beim Ausfall eines Messaufnehmers den ganzen Test neu starten muss.

Nach etwa 70 Minuten sollte alles überstanden sein. In der Praxis kam es öfter zu Störungen. In einem Fall lieferte das Ein-Phasen-Leistungsmessgerät negative Zahlen, in anderen Fällen starb eine der Messroutinen, oder der Benchmark brach während der Kalibrierung ab.

Beim Auswerten der Resultate gibt es viel zu lesen. Bei jeden Lauf entsteht ein Verzeichnis unter *Results* mit der hochgezählten Nummer im Namen, etwa *ssj.0061*, in dem Power_ssj2008 bei erfolgreichem Durchgang in 22 Dateien, Protokolle, Zwischenergebnisse, Grafiken und Endresultate sammelt. Das Hauptdokument, ein vierseitiges HTML-Dokument, krönt das, worum es die ganze Zeit ging: SPECpower_ssj2008 = 257 zum Beispiel. Eine Grafik auf der ersten Seite zeigt den Verlauf des Stromverbrauchs bei Zurücknahme der Last in 10-Prozent-Schritten.

Power im Labor erprobt

Zur Erprobung standen ein paar neue Server bereit: zwei Systeme mit AMDs Quad-Core-Opteron (Barcelona), Dells T605 OPT407 mit einem 2350 und CPIs Eagle 1413 mit vier 8350. Dem standen zwei Blades in Tarox Parx Modular Server mit Intels Xeon-CPUs gegenüber, dem E5450 und dem L5420. In erster Linie ging es darum, Varianten in der Konfiguration zu erproben, weniger um einen direkten Vergleich der Produkte [2, 3].

Beim ersten Blick in die Liste der Ergebnisse des SPECpower – Stand Mai – erscheint ausschließlich die Java-Umgebung JRockit von Bea. Allerdings in einer Power-Version, die nicht im Netz verfügbar ist. Bei der Suche nach der einst bei Bea zum Test frei erhältlichen Version steht man nun vor Oracle, das Bea übernommen habt, und findet unter den Weissagungen – nichts. Sämtliche Links auf die ehemaligen Downloads sind verschwunden. Der einzige Weg führt über Google und einige Foren, jedoch nur zur weniger performanten R-Version. Die Bevorzugung von JRockit hat Geschichte, denn ursprünglich haben die Firmen Ergebnisse des SPECjbb2005 nur mit Beas Java-Maschine erzielt.

Ende Mai taucht aber IBM mit seinem Java Runtime Environment (JRE) mit einem Build vom 3. Mai 2008 auf und legt traumhafte Zahlen vor: bis zu 1054 ops/watt auf einem Quad-Core-Xeon von Intel mit 4 GByte Hauptspeicher und Windows Server 2003 SP1 (64 Bit). Das fordert zu einer weiteren Proberunde heraus. Fujitsu Siemens ließ es sich nicht nehmen, mit JRockit auf seiner von Xeon angetriebenen Primergy TX150 S6 im Juni 2008 zu kontern und 1124 vorzulegen.

Tuningmaßnahmen fern vom Alltag

Fakt ist, dass Außenstehende die von den Herstellern publizierten Ergebnisse kaum reproduzieren können. Zum einen steht der Öffentlichkeit keine (P)-Version des JRockit zur Verfügung, zum anderen entspricht die Ausstattung der SUTs nur bedingt der Realität. Kaum jemand dürfte einen Server mit nur einer Platte betreiben. Das alleine beeinflusst zwei wesentliche Faktoren: Server im professionellen Einsatz arbeiten entweder mit mehreren lokalen Platten, nutzen einen externen Plattenstapel oder sind per SAN mit dem Speicherpool verbunden. Mal abgesehen davon, inwieweit das in die Be-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

trachtung der Energieeffizienz mit einfließen muss – schließlich stellt Software die Dienste bereit. Bei Servern im produktiven Betrieb gibt es einen Grundbedarf an Energie bedingt durch Redundanzen bei Platten und Netzteilen, Netzwerk- und RAID-Controller sowie Managementprozessoren. Hinzu kommen ständig wiederkehrende Prozesse, die für die Sicherheit des Gesamtsystems erforderlich sind, etwa Speicherabzüge hinterlegen, Backups oder Kontrollen, und die Strom verbrauchen. Benchmarks wie der SPEC power_ssj2008 entfliehen der Realität, da sie das alles nicht berücksichtigen. Der minimale Energiebedarf lag im Labor zwischen 200 und 400 Watt, bei den von den Herstellern publizierten Systemen sind es nur 52 bis 177 Watt.

Wenn dazu die per JVM frisierten *ssj_ops* kommen, entsteht schnell ein schiefes Bild: Das energetische Grundrauschen hält den Stromverbrauch hoch, nicht frisierte Warenhäuser lassen weniger Operationen pro Sekunde in dem vorgegebenen Zeitfenster über die Bühne gehen. Hinzu kommt, dass es keinerlei Profile über die typische Auslastung von Servern gibt. Im Grunde genommen gibt SPECpower_ssj2008 eine Antwort auf die Frage: Was können die eingebauten Energiesparmaßnahmen in den Servern, insbesondere in der CPU, erreichen? Wann und ob dieser Effekt zu Buche schlägt, hängt völlig vom Einsatz ab. Ein Server in der Mitte des Geschäfts, der die Datenbank trägt, dürfte kaum zur Ruhe kommen. Seine Kollegen im Terminal- oder Intranetdienst hingegen können stundenlang im wohligen Schlaf an der Energie nippen.

Fazit

Energieverbrauch zu untersuchen hat an Bedeutung gewonnen und stellt nicht nur eine neue Nuance der Benchmarks dar. Aber alle Beteiligten tun gut daran, sich kritisch mit den Resultaten und den dahinterstehenden Methoden auseinanderzusetzen. Begrüßenswert sind vor allem Bestrebungen wie die, bei der SPEC weitere Verfahren zu entwickeln, um den Energiefressern auf die Schliche zu kommen. Noch gibt es keine bunten Plaketten für IT-Systeme, die deren Umgang mit der Energie klassifizieren. Doch vorstellbar wären Sperrzonen im Netz für allzu energiehungrige oder zumindest, dass Server mit schlechter Energieeffizienz am Markt keine Chancen mehr haben. (rh)

Literatur

[1] Hubert Sieverding; Benchmarks; Wer mißt, mißt Mist; Performancemessungen im Multiprozessor-Umfeld; *iX* 10/93, S. 132

[2] Ralph Hülsenbusch; Serversysteme; RZ in 6HE; Tarox' Parx Server Center 6000R; *iX* 7/2008, S. 62

[3] Ralph Hülsenbusch; Server; Der letzte Schritt; AMDs Barcelona-CPU vom Bug befreit; *iX* 8/2008, S. 96

[4] Ralph Hülsenbusch; Benchmark; Kaufhauskette; Java Business Benchmark 2005: elektronische Warenhäuser als Test; *iX* 6/2006, S. 112

[5] Andreas Stiller; Die Vermessung der PC-Welt; Benchmark SPECpower_ssj2008 für Energieeffizienz; c't 4/08, S. 206

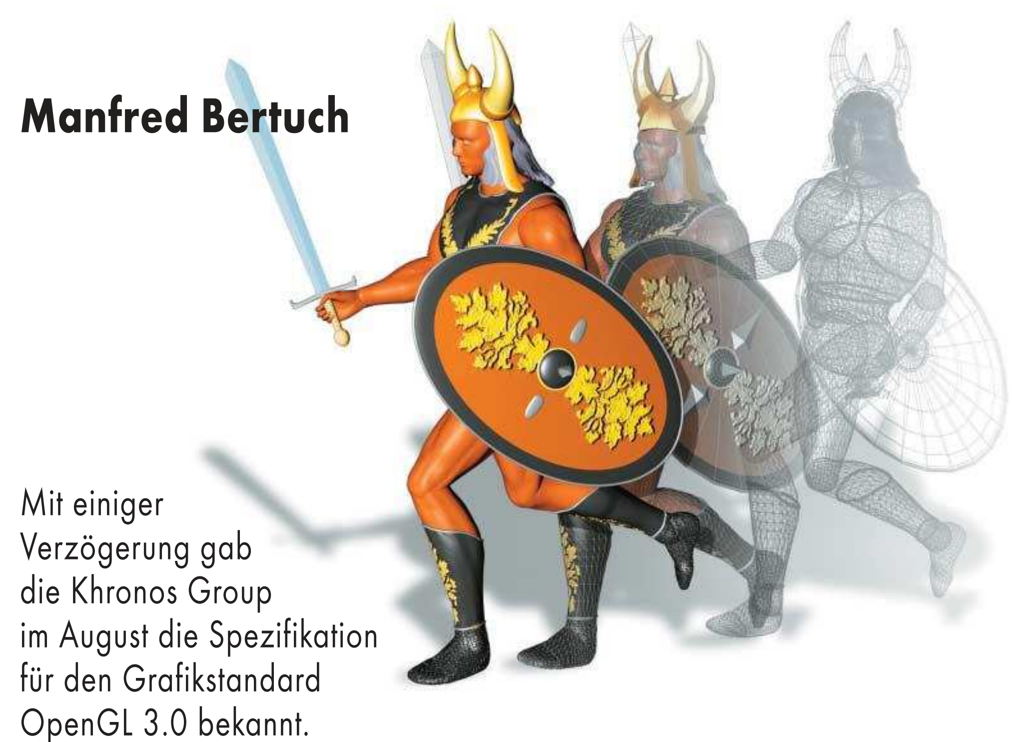


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Industriekonsortium verabschiedet OpenGL 3.0

Nachgebessert

Manfred Bertuch



Mit einiger Verzögerung gab die Khronos Group im August die Spezifikation für den Grafikstandard OpenGL 3.0 bekannt. Die 3D-Schnittstelle will damit zu Microsofts Direct3D 10 aufschließen und neue Hardwareentwicklungen auch unter OpenGL zugänglich machen.

Die unter Windows, Mac OS 9, Mac OS X, Linux und zahlreichen Unix-Varianten verfügbare Programmierschnittstelle Open GL liegt nun in der Version 3.0 vor. Sie integriert damit wesentliche Funktionen der neuen Grafikchipgeneration, die die Hersteller auf die Anforderungen von Microsofts proprietärer Grafik-API Direct3D 10 zugeschnitten haben. Die aktuellen GPUs haben neben Vertex- und Pixel-Shader (beziehungsweise Fragment-Shader) den Geometrie-Shader als neuen Typ eingeführt, können längere Shader-Programme ausführen, erhöhen die Zahl der Konstanten- und Arbeitsregister deutlich und heben viele weitere Beschränkungen auf, denen die GPUs unterliegen, die für DirectX-9 ausgelegt sind.

OpenGL 3.0 übernimmt viele der in Direct3D 10 festgelegten Funktionen sowohl in seiner Programmierschnittstelle (API) als auch in der neuen OpenGL Shading Language 1.30. GLSL 1.30 ist eine C-ähnliche Sprache, in der man Programme für die Shader-Einheiten der Grafikchips schreiben kann. Die Version 1.30 führt Ganzzahloperationen bei Texturen, Vertex- und Fragment-Shadern sowie bitweise Integer-Operationen ein. Sie fügt neue Interpolationsmodi hinzu, verbessert die Kontrolle über Textur-Operationen, bietet zusätzliche Funktionen zur Manipulation von Gleitkommazahlen und ergänzt die Flusskontrolle innerhalb von Shader-Programmen durch Switch-Statements. Schließlich verbessert GLSL 1.30 die Kompatibilität zu OpenGL ES, einer OpenGL-Variante für mobile und eingebettete Systeme.

OpenGL 3.0 selbst unterscheidet sich von seiner Vorgängerversion 2.1 in folgenden Punkten: Vertex Array Objects, nicht-blockierender Zugriff auf Vertex Buffer Objects und Verdeckungsabfragen für bedingtes Rendering sollen in erster Linie die Leistung und den Durchsatz erhöhen. Ein Feedback-Speicher erlaubt es, Geometriedaten für zusätzliche Bearbeitungsdurchgänge direkt wieder in die Vertex- und Geometrie-Shader einzuspeisen. Verbesserter Zugriff auf Frame- und Multisample-Buffer, 32-Bit-Gleitkomma-Genauigkeit bei Texturen, Render- und Tiefen-Buffer sowie Textur-Arrays ermöglichen neue Algorithmen für realistische Darstellungen und bessere Beleuchtung. sRGB-Framebuffer verbessern die Wiedergabe feiner Farbabstufungen. Den Speicherverbrauch will man dagegen mit halber Genauigkeit bei Vertex- und Pixeldaten sowie vier neuen Datenkompressionsverfahren für ein- und zweidimensionale Texturen verringern. All diese Features stammen aus Direct3D 10, weshalb man OpenGL 3.0 auch nur auf Grafikkarten mit einer sogenannten Direct3D-10-Level-GPU implementieren kann. Dies trifft gleichermaßen auf die Profi-Grafikkarten-Serien von AMD und Nvidia (FireGL und QuadroFX) zu, da sie auf denselben, ursprünglich für Direct3D ausgelegten GPUs beruhen.

Offen für neue Ideen

Weitere Neuerungen macht OpenGL über Extensions verfügbar. Hinter diesen Erweiterungen verbergen sich zusätz-

iX-TRACT

- OpenGL 3.0 und die OpenGL Shading Language 1.30 machen wichtige Funktionen neuer Grafikkarten in der Spezifikation des offenen Standards verfügbar.
- Entgegen früherer Ankündigungen des unabhängigen Herstellerkonsortiums Khronos Group bewahrt OpenGL 3.0 vollständige Abwärtskompatibilität.
- Das Deprecation-Modell von OpenGL 3.0 bereitet die Aufgabe alter Bestandteile und damit die Modernisierung der API vor.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

liche Funktionen, die nicht zur Kernspezifikation gehören. Einzelne Hersteller können sie jederzeit einführen, da sie diese nicht mit dem gesamten Konsortium abstimmen müssen. Auf diese Weise kann OpenGL schnell auf neue Entwicklungen reagieren. Die Extensions sind für eine Implementierung von OpenGL 3.0 nicht obligatorisch. Man kann aber erwarten, dass die Treiber verbreiteter Grafikkarten sie unterstützen. Nvidia stellt bereits eine Beta-Version seines OpenGL-3.0-Treibers zur Verfügung, da die Entwickler der GeForce- und QuadroFX-GPUs auch die meisten Extensions erarbeitet haben. AMD und Intel haben immerhin schon ihre Absicht erklärt, OpenGL 3.0 zu implementieren. Neuere Extensions können ebenfalls nur Grafikkarten unterstützen, die auf den Funktionsumfang von Direct3D 10 zugeschnitten sind. Im August waren bei www.opengl.org 353 Extensions registriert.

Wenn eine Extension auf größere Akzeptanz stößt, wird diese als ARB-Extension standardisiert und hat gute Aussichten, bei der nächsten Revision von OpenGL in die Spezifikation einzufließen. So waren viele Funktionen von OpenGL 3.0 ursprünglich Extensions von OpenGL 2.1. Khronos legte zudem weitere Erweiterungen für OpenGL 2.1 fest, mit denen sich einige der 3.0-Neuerungen auch mit älteren Grafikkarten nutzen lassen. Sie betreffen die Vertex-Array-, Vertex-Buffer- und die Framebuffer-Objekte, die Texturkompression, Vertices mit halber Genauigkeit sowie den sRGB-Framebuffer.

Profile schränken ein

Um OpenGL-Implementierungen zu erleichtern und zu vermeiden, dass die große Zahl der Extensions immer mitgeführt werden muss, lassen sich erstmals Profile definieren. Ein solches Profil berücksichtigt nur eine Teilmenge aller Extensions, die auf die Anforderungen einer bestimmten Anwendergruppe zugeschnitten ist. Zurzeit existiert nur ein Standardprofil, das alle Extensions umfasst. Zukünftige Versionen können dagegen spezielle Profile für Workstations, Spiele oder eingebettete Systeme einführen. Eine OpenGL-Implementierung kann sich dann auf eines dieser Profile beschränken.

Kompatibilität in beide Richtungen

Bereits vor 5 Jahren gab es mit „pure OpenGL 2.0“ einen Vorschlag, die API zu verschlanken und die Codebasis aufzuräumen, der sich aber nicht durchsetzen konnte. Auch diesmal hat die Khronos Group entgegen der ursprünglichen Ankündigung die Abwärtskompatibilität gewahrt und sämtliche Funktionen der Vorgängerversionen wieder mit aufgenommen. Das Konsortium hat lediglich Teile des Standards als veraltet erklärt (Deprecation-Modell) und signalisiert damit, dass man diese in der nächsten Version nicht mehr fortführen will. Zu den veralteten Funktionen gehören beispielsweise Pixelformate mit Farbpalette (color index mode), unterbrochene Linien (line stipple) und Linien mit einer Dicke größer als 1,0, die APIs für festverdrahtete Vertex- und Pixel-Pipelines aus der Zeit von Grafikchips für DirectX 6 und DirectX 7 sowie die Versionen 1.10 und 1.20 der Shading Language und viele weitere Funktionen aus den Anfängen von OpenGL. In der Version 3.0 kann man bereits einen vorwärtskompatiblen Kontext erzeugen, in dem die als veraltet markierten Funktionen nicht verfügbar sind.

Die Khronos Group will die weitere Entwicklung von OpenGL sowohl mit Open GL ES als auch OpenCL (Open Computing Language)

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

abstimmen. Ersteres ist eine OpenGL-Variante für mobile und eingebettete Systeme mit reduziertem Funktionsumfang. Sie ist beispielsweise auf den Spielekonsolen XBox 360 (Microsoft) und Playstation 3 (Sony) sowie auf Apples iPhone verfügbar und hat inzwischen viele proprietäre 3D-Schnittstellen ersetzt.

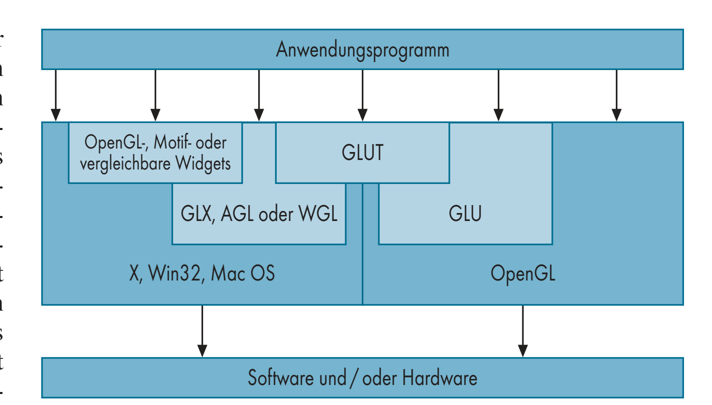
Hinter OpenCL steht ein von Apple initiierter Standard für heterogenes Rechnen auf CPUs und GPUs für technisch-wissenschaftliche und andere Anwendungen mit hohem Rechenbedarf. OpenCL soll die Last automatisch auf eine beliebige Anzahl von CPUs und GPUs verteilen können und Bestandteil des nächsten Macintosh-Betriebssystems OS X v10.6 (Snow Leopard) sein. AMD hat bereits angekündigt, die eigenen proprietären Compute-APIs wie CTM (Close To Metal) und CAL (Compute Abstraction Layer) zugunsten von OpenCL einzustellen. Nvidia will dagegen seinen eigenen Compute-Compiler CUDA (Compute Unified Device Architecture) weiterführen.

Enttäuschung bei Spieleentwicklern

Die Khronos Group wollte OpenGL 3.0, das während seiner Entwicklung unter der Codebezeichnung Longs Peak lief, ursprünglich schon im Sommer 2007 verabschieden. In der Ankündigung betonte das Konsortium noch, dass man die API verschlanken und ein neues Objektmodell einführen wolle. Das alte Objektmodell hat eine inkonsistente Semantik und ist nicht laufzeitoptimiert. Es erlaubt beispielsweise, dass sich ein Texturobjekt während seiner Benutzung von einer 2D- in eine 3D-Textur verändern kann, was natürlich das interne Objektmanagement des Grafikkartentreibers verkompliziert. Unter dem neuen Objektmodell sollte ein Texturobjekt zwar noch seinen Inhalt ändern können, aber nicht sein Format und seine Größe. Dies hätte das Treibermanagement vereinfacht, den Treiber-Overhead reduziert und damit das Laufzeitverhalten verbessert. Die alte API und das alte Objektmodell sollten trotzdem weiter verfügbar sein, um die Funktion bestehender OpenGL-Anwendungen nicht zu gefährden. Allerdings stieß das Konsortium dabei auf eine Reihe schwer lösbarer Probleme, gab dieses Vorhaben schließlich auf und entschied sich, alles beim Alten zu belassen.

OpenGL 3.0 bleibt damit hinter den Ankündigungen zurück. Es entspricht weitgehend dem Vorgänger, schleppt alle Altlasten wie den Immediate Mode und die Fixed Function Pipeline weiter mit und erklärt sie lediglich als veraltet. Es gibt auch keine Ankündigungen, das neue Objektmodell in zukünftige Versionen aufzunehmen. Einige Entwickler kritisieren zudem, dass wesentliche Features, die Direct3D 10 bereits bietet, wie Geometrie-Shader und Instanced Rendering, nicht Teil der Kernspezifikation, sondern nur über Extensions verfügbar sind. Für Unmut sorgte außerdem die spärliche Öffentlichkeitsarbeit. Während der Verzögerung gab es weder Rückmeldungen vom Konsortium noch eine Kommunikation mit der Entwicklergemeinde.

Besonders Spieleentwickler äußerten sich kritisch über OpenGL 3.0 und warfen der Khronos Group vor, zu viel Rücksicht auf die CAD-Branche und andere traditionelle Anwender zu nehmen. OpenGL würde dadurch von modernen Entwicklungen abgehängt und gerate gegenüber DirectX ins Hintertreffen. Microsoft hat mit Direct3D 10 die Kompatibilität zum Vorgänger aufgegeben und seine Schnittstelle entrümpelt. Damit muten die Redmonder den Entwicklern in der Übergangszeit zu, für zwei Schnittstellen gleichzeitig programmieren zu müssen, können aber jetzt eine übersichtliche und leistungsfähigere API vorweisen. OpenGL hat dagegen kaum noch Bedeutung in der Spielebranche, selbst wenn mit Blizzard und Transgaming noch zwei Spieleentwickler im Konsortium vertreten sind.



Die ebenfalls plattformunabhängigen OpenGL-Hilfsbibliotheken GLU und GLUT enthalten höhere Grafikfunktionen sowie eine allgemeine Fenstersteuerung. GLX, AGL und WGL binden Letztere an das jeweilige Betriebssystem an.

Fazit

OpenGL 3.0 ist vollständig abwärtskompatibel, und sämtliche bestehende OpenGL-Anwendungen sind unter der neuen Version unverändert lauffähig. Damit bewahrt der 3D-Standard seine vielleicht größte Stärke: die Stabilität der Schnittstelle. Aber nach 15 Jahren wird es immer schwieriger, neue Konzepte in OpenGL zu integrieren ohne Altlasten aufzugeben. Die Khronos Group musste einige ihrer ursprünglichen Pläne verwerfen, und der Sprung von OpenGL 2.1 nach 3.0 ist weit weniger radikal ausgefallen, als der von OpenGL 1.5 nach 2.0. Aber das Deprecation-Modell der Version 3.0 bereitet den harten Schnitt vor. Auch wenn die Khronos Group diesen nicht konkret ankündigt, ist er mit der nächsten größeren Revison wohl unvermeidlich. Andernfalls verliert OpenGL durch mangelnde Übersicht und Konsistenz unweigerlich an Attraktivität. (ka)

MANFRED BERTUCH

war langjähriger Redakteur der c't und arbeitet jetzt als freier Autor für die Themengebiete Grafik und Multimedia in Berlin.

Onlinequellen

OpenGL-Spezifikationen	www.khronos.org/opengl/
OpenGL-Hintergrund und Programmierung	www.opengl.org
Beta-OpenGL-3.0-Treiber von Nvidia	developer.nvidia.com/object/opengl_3_driver.html
Hitler Not Impressed With OpenGL 3.0	www.youtube.com/watch?v=sddv3d-w5p4

Literatur

[1] Manfred Bertuch; Standards für virtuelle Welten; Die Grafikschnittstellen OpenGL 2.0 und Direct3D 9.0; *iX* 4/03, S. 105

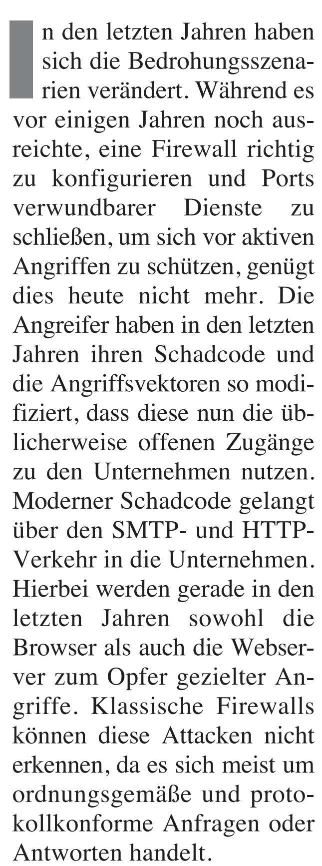
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Apaches Web Application Firewall Modsecurity

Feuerwand für den Indianer

Ralf Spenneberg

Gegen „moderne“ Attacken – beispielsweise via Cross-Site Scripting oder Javascript Hijacking – bieten nur sogenannte Web Application Firewalls wirksamen Schutz. Das für den Apache Webserver entwickelte Modsecurity ist der bekannteste Open-Source-Vertreter dieser Gattung.



In den letzten Jahren haben sich die Bedrohungsszenarien verändert. Während es vor einigen Jahren noch ausreichte, eine Firewall richtig zu konfigurieren und Ports verwundbarer Dienste zu schließen, um sich vor aktiven Angriffen zu schützen, genügt dies heute nicht mehr. Die Angreifer haben in den letzten Jahren ihren Schadcode und die Angriffsvektoren so modifiziert, dass diese nun die üblicherweise offenen Zugänge zu den Unternehmen nutzen. Moderner Schadcode gelangt über den SMTP- und HTTP-Verkehr in die Unternehmen. Hierbei werden gerade in den letzten Jahren sowohl die Browser als auch die Webserver zum Opfer gezielter Angriffe. Klassische Firewalls können diese Attacken nicht erkennen, da es sich meist um ordnungsgemäße und protokollkonforme Anfragen oder Antworten handelt.

Daher bedarf es neuer Abwehrmaßnahmen. Speziell für den Schutz von Webservern und den darauf betriebenen Applikationen entstanden die Web Application Firewalls (WAF). *iX* befasste sich in der Ausgabe 8/2008 [1] ausführlich mit den kommerziellen WAFs von Herstellern wie Barracuda Citrix, F5 oder Imperva – um nur einige zu nennen –, die häufig fünfstellige Summen für ihre Produkte verlangen. Modsecurity (siehe „Onlinequellen [a]) ist einer der prominentesten Open-Source-Vertreter dieser Gattung, der in der Praxis häufig zum Einsatz kommt.

Vorteile durch die Nähe zu Apache

Ivan Ristic entwickelte Modsecurity über die letzten Jahre als Open-Source-Modul für den Apache Webserver – ursprünglich für die Version 1.3. Die aktuellen Releases – inzwischen ist 2.5.6 aktuell – unterstützen jedoch nur noch Apache 2.x. Ristic verfügt über jahrelange Erfahrung im Bereich der Webserversicherheit. Sein Buch „Apache Security“ [2] war eines der ersten Bücher zu diesem Thema. Seit Jahren engagiert er sich im Web Application Security Consortium [b] und ist hier verantwortlich für die Web Application Firewall Evaluation Criteria. Im September 2006 übernahm Breach Security [c] Ristics Firma Thinking Stone. Modsecurity ist seitdem sowohl unter einer Open-Source- als auch einer kommerziellen Lizenz verfügbar.

Da Modsecurity als Modul im Apache arbeitet, kann es dessen kompletten Funktionsumfang nutzen. Das hilft beispielsweise bei der Analyse SSL-verschlüsselten Verkehrs, da diese nach der Entschlüsselung durch *modssl* erfolgt. Auch lässt sich die freie WAF auf allen von Apache unterstützten Betriebssystemen einsetzen, also einschließlich Windows oder BSD. Darüber hinaus entsteht kein weiterer Overhead für die Netzwerkkommunikation und nur ein geringer zusätzlicher Overhead für das Parsing. Will man einen anderen Webserver als Apache schützen, so kann Modsecurity – im Gespann mit einem als Reverse-Proxy konfigurierten Apache – dennoch den Verkehr analysieren und so die Webanwendung schützen.



Alles eine Frage des Regelwerks

Zum Lieferumfang gehört ein umfangreiches Regelwerk, das mit regulären Ausdrücken die übergebenen Daten und Parameter prüft und die heute typischen Angriffe erkennt. Diagnostiziert Modsecurity einen Angriff, kann der Administrator entscheiden, ob er den Zugriff verbietet oder lediglich protokolliert. Diesem Ansatz liegt ein Known-Weaknesses-Modell zugrunde. Modsecurity arbeitet hier wie ein Virenscanner, der alle Zugriffe auf bekannte Schwä-



iX-TRACT

- Modsecurity ist die einzige ernst zu nehmende Open-Source-Variante einer Web Application Firewall, die auch in produktiven Umgebungen ausreichend Schutz bietet.
- Anpassungen der freien WAF an die eigenen Bedürfnisse erfolgen über Regeln mit regulären Ausdrücken.
- Über Verkettungen von Regeln lassen sich auch komplexe Sachverhalte sicher überprüfen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Was Modsecurity nicht kann

Im Gegensatz zu den kommerziellen WAF fehlen Modsecurity einige Funktionen. So kennt es keine Cookie-Verschlüsselung, die eine Modifikation oder einen Diebstahl von Cookies verhindern könnte. Auch ein Lernmodus für die Ermittlung der erlaubten Wertebereiche der übergebenen Parameter einer Webapplikation fehlt. Diese muss der Systemverwalter manuell bestimmen und in Form von Regeln konfigurieren. Genauso fehlt ein Lernmodus, der das Surfverhalten nachbildet und so einen direkten Zugriff auf bestimmte Seiten verbietet. Angreifer nutzen meist Skripte, die direkt mehrfach nacheinander automatisch verwundbare Seiten aufrufen. Dies kann Modsecurity aktuell nicht erkennen und daher nicht verhindern. Allerdings nutzen auch kommerzielle WAFs diese Funktion häufig nicht, da dies ein Deep Linking und Bookmarking durch die Benutzer verbietet.

chen prüft. Alternativ kann der Systemverwalter mit höherem Konfigurationsaufwand Modsecurity in zwei alternativen Modellen betreiben. Er kann sein eigenes Regelwerk so gestalten, dass es alle Zugriffe erkennt, die die Webapplikation zum Funktionieren benötigt. Modsecurity konfiguriert er dann so, dass es nur diese Zugriffe erlaubt und alle anderen unterbindet. Ist dem Admin eine ungepatchte Sicherheitslücke der Webapplikation bewusst, kann er alternativ eine Regel schreiben, die genau diesen Zugriff erkennt und verbietet. Dies ist hilfreich, wenn der Hersteller rechtzeitig keinen Patch zur Verfügung stellen kann oder will.

Für das Schreiben dieser Regeln muss der Systemverwalter lediglich reguläre Ausdrücke beherrschen. Viele Administratoren entmutigt jedoch der erste Blick auf die mitgelieferten Regeln, Listing 1 zeigt ein Beispiel. Diese scheinen zunächst unglaublich kompliziert. Ziel dieser Regeln ist es, möglichst viele reguläre Ausdrücke gleichzeitig zu testen. Dies erhöht die Ausführungsgeschwindigkeit enorm. Da diese Komprimierung von Hand kaum durchführbar ist, ist es sinnvoll, hierfür ein kleines Perl-Skript zu verwenden. Das Skript in Listing 2 nimmt mehrere reguläre Ausdrücke über die Standard-Eingabe entgegen und komprimiert diese über die Perl-Bibliothek *Regexp::Assemble* wie in den Modsecurity-Regeln.

Über selbstgeschriebene Regeln kann der Admin genau festlegen, wann Modsecurity Alarm schlagen soll. Dabei lassen sich jeder einzelne übergebene Parameter und alle Daten überprüfen.

Modsecurity teilt jede Transaktion in 5 Phasen ein:

1. *REQUEST_HEADERS*
2. *REQUEST_BODY*
3. *RESPONSE_HEADERS*
4. *RESPONSE_BODY*
5. *LOGGING*

Listing 1: Mitgelieferte Filterregeln

```
SecRule REQUEST_FILENAME|ARGS|ARGS_NAMES|REQUEST_HEADERS|XML:/*|!REQUEST_HEADERS:Referer
"@pm sys.user_triggers sys.user_objects @@spid msysaces instr sys.user_
views sys.tab charindex sys.user_catalog constraint_type locate select msysobjects
attnotnull sys.user_tables sys.user_tab_columns sys.user_constraints waitfor
mysql.user sys.all_tables msysrelationships msyscolumns msysqueries" \
       "phase:2,t:none,t:urlDecodeUni,t:htmlEntityDecode,t:lowercase,t:replace
Comments,t:compressWhiteSpace,pass,nolog,skip:1"
SecAction phase:2,pass,nolog,skipAfter:959007
SecRule REQUEST_FILENAME|ARGS|ARGS_NAMES "(?:\b(?:(?:s(?:ys\.(?:user_(?:(?:t(?:ab
(?:_column|le)|rigger)|object|view)s|c(?:onstraints|atalog))|all_tables|tab)|el
ect\b.{0,40}\b(?:substring|ascii|user))|m(?:sys(?:(?:queri|ac)e|relationship|column|
object)s|ysql\.user)|c(?:onstraint_type|harindex)|waitfor\b\W*?\bdelay|attnotnull)\b|
(?:locate|instr)\W+\()|\@\@spid\b)" \
       "phase:2,capture,t:none,t:htmlEntityDecode,t:lowercase,t:replaceComments,t:
compressWhiteSpace,ctl:auditLogParts=+E,deny,log,auditlog,status:501,msg:'Blind SQL
Injection Attack',id:'950007',tag:'WEB_ATTACK/SQL_INJECTION',logdata:'%{TX.0}',severity:'2'"
```

Bei der Definition der Regeln kann der Admin festlegen, in welchen Phasen sie greifen soll. Einige Informationen stehen nur in bestimmten Phasen zur Verfügung. In der ersten Phase analysiert Modsecurity die Header der HTTP-Anfrage. Hierbei verwendet es soweit möglich die Daten des Apache. Anschließend puffert und untersucht es den Body der Anfrage. Im nächsten Schritt erfolgt die Auswertung der Regeln der zweiten Phase. Nun darf der Webserver die Anfrage verarbeiten. Bevor der Apache seine Antwort sendet, prüft Modsecurity die Regeln der Phase 3 und analysiert die Header. In Abhängigkeit seiner Konfiguration puffert Modsecurity den Body der Antwort, um auch diesen in Phase 4 zu prüfen. Da sich die meisten Angriffe in den Request-Headern und -Body finden, kann der Admin dies konfigurieren. Nach der Phase 4 darf der Apache seine Antwort versenden. In der Phase 5 protokolliert Modsecurity seine Ergebnisse. Wenn gewünscht, kann es auch die gesamte Transaktion für forensische Zwecke protokollieren.

Für die Definition der Regeln verwendet Modsecurity eine einfache Sprache, die Bestandteil der Apache-Konfiguration ist. Die generische Syntax entspricht: *SecRule TARGETS OPERATOR [ACTIONS]*. Ein Beispiel für eine einfache Regel mag sein:

```
SecRule ARGS|REQUEST_HEADERS ⁊
                    "@rx <script"
"id:1000001,msg:'Cross-Site-Scripting', ⁊
        severity:ERROR,deny,phase:2, ⁊
                       status:500"
```

Mithilfe der Variablen *ARGS* und *REQUEST_HEADERS*

Listing 2

```
#!/usr/local/bin/perl
use strict;
use Regexp::Assemble;

my $ra = Regexp::Assemble->new;
while (<>)
{
  $ra->add($_);
}
print $ra->as_string() . "\n";
```

definiert der Admin, wo Modsecurity suchen soll. Aktuell stehen 78 Variablen zur Verfügung, die jede erdenkliche Information bereitstellen. Damit Modsecurity auch weiß, mit welchem Algorithmus die Suche erfolgen soll, gibt der Admin diesen mit 22 verschiedenen Operatoren an. *@rx* realisiert die Suche mit einem regulären Ausdruck während *@eq* und *@lt* numerische Vergleiche durchführen (*equal*, *less than*). Ist kein Operator angegeben, verwendet Modsecurity *@rx* als Default. Schließlich bestimmt die Regel auch, wie sich Modsecurity bei einer erfolgreichen Suche verhalten soll. 42 unterschiedliche Aktionen (*deny*, *log* et cetera) erlauben den Abbruch der Verbindung, die Protokollierung, das Setzen von internen Variablen und vieles mehr.

Anwendung in der Praxis

Bei der Anwendung von Modsecurity, sollte der Admin zunächst prüfen, ob eine Analyse aller Zugriffe auf den Webserver tatsächlich erforderlich ist. In vielen Fällen gibt es Verzeichnisse, die statische Daten (Bilder) enthalten und die man ausnehmen kann, um unnötige Bearbeitungszeit zu sparen.

```
<Location /images/>
  SecRuleEngine Off
</Location>
```

Sind die Bilder über viele Verzeichnisse verteilt, kann sich der Admin mit folgendem Konstrukt helfen:

```
SecRule REQUEST_BASENAME ⁊
     "\.(png|jpg)$" chain,allow,nolog
SecRule REQUEST_METHOD ⁊
                 "^(GET|HEAD)$" chain
SecRule &ARGS "@eq 0"
```

Hier prüft Modsecurity zunächst, ob die angeforderte Datei auf *.png* oder *.jpg* endet. Anschließend prüft Modsecurity, ob als Methode *GET* oder *HEAD* dienen und die Anzahl der Argumente *null* ist. Das

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Schlüsselwort *chain* verkettet die Regeln. Mit *allow,nolog* in der ersten Regel erlaubt der Admin den Zugriff, wenn alle Regeln zutreffen, und deaktiviert die Protokollierung.

In vielen Fällen möchte man einen Client vielleicht nicht bei der ersten Erkennung abweisen. Ähnlich dem Verhalten von Spamassassin möchte er auch mehrere Aspekte prüfen und nur, wenn drei von fünf Prüfungen erfolgreich waren, den Zugriff verhindern. Dies lässt sich auch mit Modsecurity realisieren. Hierzu muss es jedoch Informationen über die IP-Adresse speichern. Modsecurity bezeichnet dies als Collection. Die Initialisierung erfolgt in der Phase 1:

```
SecAction "phase:1,initcol:ip=% ↵
        {REMOTE_ADDR},nolog,pass"
```

Anschließend schreibt der Admin seine Regeln so, dass Modsecurity bei einem Treffer eine IP-abhängige Variable hochzählt:

```
SecRule ARGS "<script"
"phase:2,pass,setvar:ip.score=+1"
```

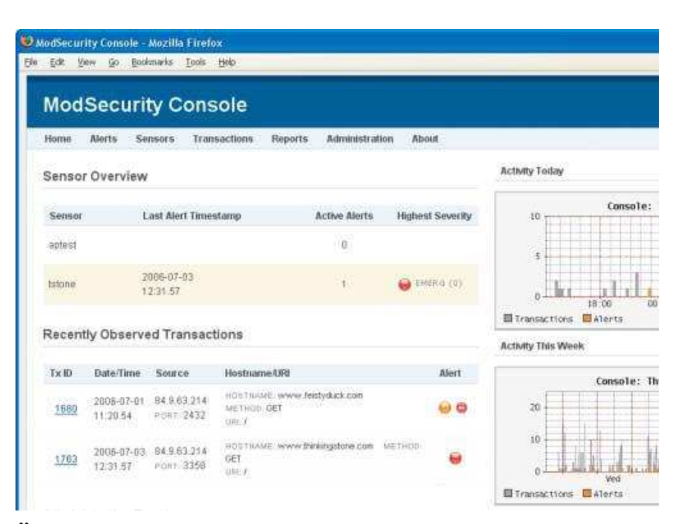
Treffen nun mehrere derartige Regeln zu, beträgt der Score am Ende 3 und Modsecurity lehnt weitere erneute Zugriffe von der IP-Adresse ab.

```
SecRule IP:score "@gt 2"
"phase:1,log,deny"
```

Ähnlich lassen sich auch Sessions überwachen. Hier ist die Collection *SESSION* jedoch schon vorbereitet und lässt sich einfach verwenden:

```
SecRule
REQUEST_COOKIES:PHPSESSID
"!^$" "chain,phase:2,nolog,pass, ↵
 setsid:%{REQUEST_COOKIES.PHP ↵
                         SESSID}"
```

Diese Möglichkeiten nutzen die mitgelieferten Regeln im Moment kaum, da ihre Verwendung spezielle Kenntnisse über den Aufbau der Webapplikation erfordert. Der Anwender kann damit die zur Verfügung gestellten Regeln aber an seine eigenen Anforderungen anpassen.



Über die kostenlose Modsecurity-Konsole kann der Administrator die abgewehrten Angriffe analysieren (Abb. 1).

Verbesserte Performance

Reguläre Ausdrücke sind nicht gerade für ihre Geschwindigkeit berühmt, was in der Vergangenheit zu Performanceproblemen beim Einsatz von Modsecurity führte. Seit der Version 2.5 verfügt Modsecurity über den Pattern-Matching-Algorithmus von Aho-Corasick [d], mit dem es sehr schnell nach festen Zeichenketten suchen kann. Der Algorithmus bildet auch die Grundlage des Unix-Kom-



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

mandos *fgrep*. Die Regeln passten die Entwickler nun so an, dass Modsecurity zunächst schnell nach bestimmten Zeichenketten sucht. Tauchen diese nicht auf, kann es sich auch nicht um den dazugehörigen Angriff handeln. Im positiven Fall prüft Modsecurity mit regulären Ausdrücken in weiteren Regeln, ob es sich tatsächlich um den Angriff handelt, in dem es den Kontext überprüft. Dies ist auch in den Regeln aus Listing 1 zu erkennen. Mit der ersten prüft Modsecurity per Pattern-Matching (*@pm*), ob die Zeichenketten vorhanden sind. Falls ja, überspringt es die folgende Regel (*skip:1*) und testet genauer mit regulären Ausdrücken. Falls nein, überspringt Modsecurity in der nächsten Regel den Block mit den regulären Ausdrücken und führt den nächsten Pattern-Matching-Test durch. Mit diesem Mechanismus konnte Modsecurity 2.5 seine Verarbeitungsgeschwindigkeit gegenüber der Version 2 in Abhängigkeit der eingesetzten Regeln um den Faktor zwei bis fünf beschleunigen.

Ein Stück zurückgerudert

Eine weitere Verbesserung von Modsecurity 2.5 in puncto Geschwindigkeit versprach das aggressive Caching von normalisierten Daten. Modsecurity normalisiert sämtliche Anfragen, um das Schreiben der regulären Ausdrücke zu vereinfachen. So dekodiert es beispielsweise zunächst alle Anfragen in Listing 1 (*urlDecodeUni*, *htmlEntityDecode*), wandelt sie in Kleinbuchstaben um (*lowercase*) und entfernt schließlich mehrfache Leerzeichen und Kommentare (*compressWhiteSpace*, *replaceComments*). Die Ergebnisse dieser Transformationen speichert Modsecurity heute aggressiv zwischen. In der Vergangenheit führte es alle Transformationen für jede Regel erneut durch. Leider hat sich genau dieses Caching-Subsystem als sehr instabil und fehlerhaft herausgestellt, sodass die Entwickler es in der aktuellen Version 2.5.6 deaktiviert haben und ihm den Status *deprecated* zuwiesen.

Darüber hinaus bietet Modsecurity Verbesserungen, die sich heute noch nicht richtig abschätzen lassen. So verfügen die aktuellen Versionen über ein Skript (*rules-updater.pl*) für ein automatisches Regel-Update. Leider existiert noch kein Repositorium, von dem es die Regeln laden könnte. Dies soll bei Breach Security gehostet werden.

Neuerungen mit viel Potenzial

Eine weitere Neuerung ist die Fähigkeit, beliebigen Inhalt in die ausgelieferten Seiten einzufügen. Auch hier fehlen im Moment noch die richtigen Ideen und Anwendungen, was sicherlich mit den im derzeitigen Status eher rudimentären Möglichkeiten zusammenhängt. Breach Security plant jedoch hier eine mächtige Schnittstelle zu schaffen, mit der sich der Content vor der Auslieferung beliebig modifizieren lässt. So könnte Modsecurity bei einem potenziellen Angriff durch Einschleusen von entsprechendem Javascript-Code ermitteln, ob die Gegenstelle ein Javascript-fähiger Browser ist oder ob es sich um ein Hacking-Tool handelt, das Javascript nicht auswertet.

Genauso erschließt die Einbindung der Skriptsprache Lua in Modsecurity noch ungeahnte Möglichkeiten. Lua ist vielen Anwendern von World-of-Warcraft als schnelle Skriptsprache für die GUI-Entwicklung bekannt. Aber auch andere bekannte Programme verwenden Lua: Nmap, Wireshark, Prelude-IDS-Correlator und Snort ab Version 3.0. Der Admin kann nun in Lua beliebige Skripte schreiben, die auf sämtliche Modsecurity verfügbaren Informationen zugreifen können, die die freie WAF direkt auswertet. Darüber lassen sich komplexe Prüfungen realisieren, die in Modsecuritys Sprache nicht abbildbar sind.

So kann Modsecurity mit dem Schlüsselwort *chain* gut Und-Verknüpfungen abbilden. Oder-Verknüpfungen sind jedoch problematisch. Außerdem kann der Admin in dem Lua-Skript auch Berechnungen durchführen, die über einen einfachen numerischen Vergleich hinausgehen.

Setzt man Apache auch zum Upload von Dateien ein, kann Modsecurity diese zunächst in einem temporären Verzeichnis sichern und mit einem Virenscanner prüfen, bevor die Webapplikation Zugriff darauf erhält.

Überwachung wahlweise grafisch

Modsecurity protokolliert seine Meldungen in einer Textdatei. Deren Analyse ist aufwendig – sie muss per Hand erfolgen – und verbleibt daher oft. Hier sieht Breach Security sein kommerzielles Potenzial. Zunächst stellt Breach Security ein GUI bereit, die Modsecurity-Konsole. Wie Abbildung 1 zeigt, bietet sie eine grafische Sicht auf erkannte und verhinderte Angriffe.

Ohne Lizenzzahlung kann die Software bis zu drei Modsecurity-Instanzen (Sensoren) überwachen und verwalten. Hierzu muss man nach der Registrierung über die Breach Security Website eine kostenlose Lizenz anfordern.

Fazit

Vor allem die vielen Funktionen und der einfache Einsatz unter Verwendung der mitgelieferten Regeln sprechen für Modsecurity. Zusätzliche Fähigkeiten, wie der einfache Betrieb des Apache in einer *chroot*-Umgebung und die Option, die Apache-Kennung in der Serverantwort auf einen beliebigen Wert zu setzen, sprechen sicherlich für den Einsatz von Modsecurity. Ob diese Argumente die Schwachstellen (siehe Kasten „Was Modsecurity nicht kann“) überwiegen, und es sich daher für den eigenen Webserver eignet, muss jeder selbst entscheiden. Einige große Webportale nutzen es jedoch zur Verbesserung ihrer Sicherheit. (avr)

RALF SPENNEBERG

ist als Trainer und Berater seit vielen Jahren im Linux- und Unix-Umfeld tätig. Seit 2005 führt er mit seinem Unternehmen Open Source Training Ralf Spenneberg auch Schulungen durch.

Literatur

[1] Michael Dipper, Andreas Kurtz; Websicherheit; Bevor es brennt; Acht Web Application Firewalls; *iX* 8/2008, S. 70

[2] Ivan Ristic; Apache Security; First Edition; ISBN 978-0-596-00724-9; O'Reilly 2005

[3] Ryan C. Barnett; Preventing Web Attacks with Apache; ISBN 978-0-321-32128-2; Addison-Wesley Longman, Amsterdam 2006





Onlinequellen

[a]	Modsecurity	www.modsecurity.org
[b]	Web Application Security Consortium	www.webappsec.org
[c]	Breach Security	www.breach.com
[d]	Aho-Corasick	en.wikipedia.org/wiki/Aho-Corasick_algorithm

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Performante und gesicherte virtuelle Laufwerke für VMs

Wolkenschicht

Sven Ahnert

Ob bei der Virtualisierung produktiver Server im Rechenzentrum oder in Testumgebungen auf dem Laptop – virtuelle Festplatten sind die „Seele" virtueller Maschinen. Sie bestimmen maßgeblich Leistung, Handhabung und Funktion der Gäste.

Aus Anwendersicht definiert sich eine virtuelle Maschine (VM) hauptsächlich über den Inhalt ihrer Datenträger, denn dort liegen die installierten Gastsysteme samt Applikationen und Daten. Virtuelle Platten (Vdisks) bilden sozusagen den Lebensnerv eines Gastes, alle anderen Komponenten sind ersetzbar: Verlorene Konfigurationsdateien einer VM kann der Anwender mit wenigen Mausklicks neu erstellen, Konvertierungswerkzeuge ermöglichen den unkomplizierten Wechsel des Virtualisierers und selbst bei ausgefallener Hardware starten Gäste auf einem anderen Host. Dagegen zieht der Verlust einer Vdisk, etwa durch versehentliches Löschen, den Totalausfall und das Verschwinden des Gastsystems nach sich.

Zudem spielen sie eine entscheidende Rolle für die Leistung der Gäste, denn Datenträger und ihre Anbindungen bilden für VMs häufig den Flaschenhals, noch vor CPU und Hauptspeicher. Kenntnisse im Umgang mit Vdisks und der Planung der Speicheranbindung sind für den reibungslosen Betrieb einer virtuellen Umgebung unerlässlich.

Ein großer Vorteil virtueller gegenüber physischen Festplatten liegt in der praktischen Handhabung. So lassen sich die Gastsysteme durch einfaches Kopieren der Vdisks sichern und wiederherstellen. Genauso kann ein Entwickler fertige Demo-Umgebungen auf DVD brennen und an Kunden schicken. Nicht zuletzt bieten Vdisks Funktionen wie Snapshots und schnelles Klonen.

Prinzipiell ähneln sich die Konzepte und der Aufbau virtueller Platten bei allen Virtualisierern, von VMware über Xen bis zu Microsofts Virtualisierungsprodukten: Der Virtualisierungslayer fängt die Plattenzugriffe der Gastsysteme ab und leitet sie in eine Containerdatei um, die auf dem Dateisystem des Host liegt. Sie umfasst den Inhalt aller Sektoren, die das Gastsystem schreibt. Jede Vdisk ist eine separate Datei, die dem Gast als normale Festplatte erscheint – das Betriebssystem in der VM bemerkt von diesem Trick nichts.

Dateien statt Peripherie

Der Virtualisierungslayer emuliert in der VM einen weit verbreiteten IDE- oder SCSI-Controller, etwa von LSI Logic oder Adaptec, für den die meisten Gastsysteme Treiber mitbringen. Einige Virtualisierer stellen optimierte Festplattentreiber bereit, die deren Leistung verbessern sollen. Die Gäste benötigen dann keine Treiber für die reale Hardware, etwa für RAID-Controller oder HBAs, da deren Ansteuerung der Host übernimmt. Dadurch spielt es prinzipiell keine Rolle, ob das Dateisystem eines Gasts auf einer billigen IDE-Platte oder im Fibre-Channel-SAN liegt.

Grundsätzlich kann man virtuelle Platten aus zwei Perspektiven betrachten: aus Sicht des Host und aus Sicht des Gastsystems. Für den Host sind es einfach große Dateien mit den Endungen **.vmdk* oder **.vhd* (siehe Kasten „Dateien virtueller Platten"), die auf einem verfügbaren Datenträger liegen. Als Ablageplatz genügen in

iX-TRACT

- Virtuelle Platten bieten einen flexiblen Umgang mit den Gastsystemen, wie es mit physischen Festplatten kaum denkbar wäre.
- In größeren Umgebungen mit mehreren Hosts verlagert man die virtuellen Platten ins Speichernetz. Dadurch lassen sich die Gäste jederzeit zwischen den Hosts verschieben.
- Beachten sollte man auf jeden Fall die Verteilung der einzelnen virtuellen Disks auf die physikalischen beziehungsweise RAID-Sets und Volumes, da man sich sonst schnell Performance-Engpässe einhandelt.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Testumgebungen lokale IDE- oder SATA-Platten, externe USB-Laufwerke oder exportierte Verzeichnisse im LAN. USB-Laufwerke eignen sich für den Transport virtueller Maschinen, zur preiswerten Archivierung oder als Ergänzung von Laptops mit kleinen Festplatten. Zum produktiven Einsatz eines Host dienen lokale RAID-Sets oder zugewiesene Volumes im SAN.

Hosted oder Bare Metal

Bei den Hosted-Virtualisierern, die als Anwendungen auf einem vorhandenen Linux oder Windows laufen, kann man die Datenträger frei wählen. Hierzu zählen VMwares Workstation und Server oder Microsofts Virtual PC und Server. Die VMs können durch die breite Geräteunterstützung des Wirtssystems auf allen Datenträgern liegen, die am Host als Laufwerke erscheinen – selbst auf einem USB-Stick oder MP3-Player.

Citrix' Xen und Microsofts Hyper-V sind zwar sogenannte Bare-Metal-Virtualisierer, sie nutzen aber die Treiber eines Basis-Systems, das in der Domain 0 beziehungsweise der Parent-Partition läuft. Dadurch kommen diese Virtualisierer ebenfalls in den Genuss der gesamten Datenträgerunterstützung von Linux respektive Windows Server 2008.

VMwares ESX-Server – der als Bare-Metal-Virtualisierer sein eigenes Betriebssystem gleich mitbringt – steuert die physische Hardware mit seinen eigenen Treibern an. Red Hats Linux in der Servicekonsole dient nur der Verwaltung, Linux-Treiber haben keinen Zugriff auf die physischen Komponenten. Das erfordert aber für den ESX-Server zertifizierte Hardware. Dafür hat VMware die Controller-Treiber optimiert und viele Funktionen wie Multipathing oder Clustering integriert. Der Preis: Der ESX-Server unterstützt als Ablageplatz für Vdisks zwar lokale SCSI- und SATA-Festplatten beziehungsweise RAID-Sets, allerdings keine IDE-Platten. Als externer Speicher dienen per iSCSI oder Fibre Channel angebundene Volumes im SAN oder per NFS freigegebene Verzeichnisse.

Beim Fibre Channel und iSCSI unterstützt ESX Server redundante Pfade zwecks Failover bei Verbindungsausfall. Für eine preiswerte Speicheranbindung in kleineren Umgebungen integriert ESX Server einen Software-iSCSI-Initiator, der seine SCSI-Kommandos über die Ethernet-Ports schickt. Damit können teure iSCSI-HBAs entfallen, allerdings auf Kosten der Host-CPU und damit – je nach ihrer Auslastung – mit leichten Abstrichen bei der Performance. Für Software-iSCSI und NFS ermöglicht ESX das Teaming (Gruppieren) mehrerer Netzwerkkarten zur Ausfallsicherheit.

Schlüssel zur Flexibilität

Lokale Datenträger und SAN-Volumes formatiert VMwares ESX Server mit dem optimierten Dateisystem VMFS. Auf NFS-Freigaben liegen die Vdisks dagegen direkt im Dateisystem des NAS- oder Fileservers.

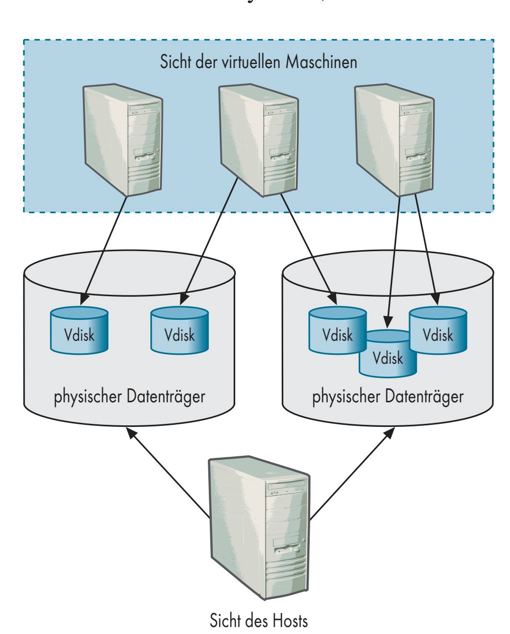
In produktiven Umgebungen befinden sich die Vdisks der Gäste meist auf externem Speicher, etwa auf einem per SCSI-LUN zugänglichen Volume im SAN. Da VMFS clusterfähig ist, können mehrere ESX Hosts gleichzeitig auf eine LUN respektive das Volume zugreifen. Diese Fähigkeit ermöglicht das flexible Verteilen von VMs auf unterschiedliche Hosts, ohne die virtuellen Platten jedes Mal zu kopieren oder LUNs zwischen den Hosts neu zuzuweisen. Ohne VMFS funktioniert der gemeinsame Zugriff nur auf NFS-Freigaben.

Andere Produkte, etwa Microsofts Virtual Server oder der in den Windows 2008 Server integrierte Hyper-V, agieren nicht so flexibel mit im Netz liegendem Storage [1]. Microsoft beherrscht durch seine Clusterdienste zwar ebenfalls das Verschieben von VMs zwischen den Hosts, aber nur für ganze Partitionen samt aller enthaltenen Gäste. Schuld daran ist NTFS, weil es nicht für den simultanen Zugriff mehrerer Rechner ausgelegt ist und explizit einem Server zugeordnet sein muss. Dadurch laufen immer alle VMs eines Volumes auf dem gleichen Host. Eine Alternative kann bei Hyper-V die Ablage auf SMB/CIFS-Freigaben eines Fileservers sein.

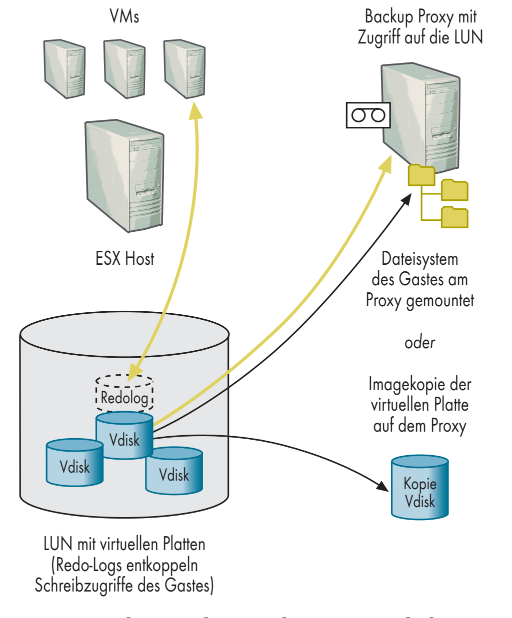
Netzspeicher ermöglicht Funktionen zur Live-Migration von Gästen mit VMwares VMotion, XEN-Motion oder etwas eingeschränkt mit Microsofts Quick-Migration. Das gewährleistet optimale Lastverteilung der VMs und erlaubt das Verschieben von VMs zwischen den Hosts für Wartungszwecke im laufenden Betrieb. Auch der automatische Neustart von Gästen auf einem anderen Wirt bei Host-Ausfällen gelingt nur, wenn die Vdisks auf einem für beide zugreifbaren Speicher liegen.

Gerechte Platzverteilung

Bereits die Planung der Kapazität der Vdisks entscheidet über die spätere Leistung der virtuellen Umgebung. In Testumgebungen, etwa mit VMware Workstation oder



Containerdateien der Vdisks können auf unterschiedlichen physischen Datenträgern liegen (Abb. 1).



Netzspeicher und Snapshots ermöglichen Hot-Backups der Gäste direkt vom SAN (Abb. 2).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

MS Virtual PC, sollte man die VMs möglichst vom Host-System trennen, damit sich deren Zugriffe nicht gegenseitig behindern. Im einfachsten Falle enthält eine Festplatte das Host-System, und eine weitere nimmt die VMs auf.

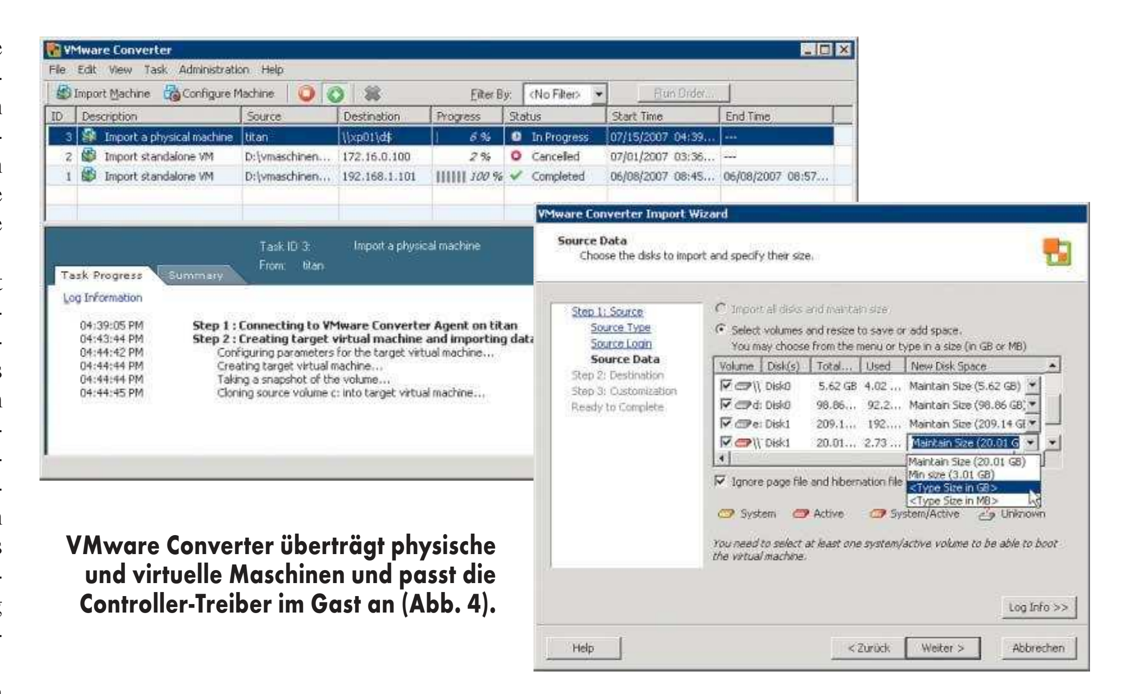
Diese Trennung gilt erst recht für kleinere Produktivumgebungen mit lokalen Platten. Hier kann ein kleines Spiegel-Set das Hostsystem aufnehmen und ein RAID-5- oder RAID-10-Set die virtuellen Maschinen. In Umgebungen mit mehreren Hosts liegen die VMs im Speichernetz, was Fragen nach der Speicheranbindung und der Aufteilung des verfügbaren Platzes aufwirft.

Bei großen Umgebungen dominiert Fibre Channel mit 2 oder 4 GBit/s. Dagegen kann sich iSCSI für bestimmte kleine und mittlere Umgebungen eignen. NFS-Server als zentraler Speicherort für VMs sind ebenfalls auf dem Vormarsch. Ihr Vorteil liegt darin, dass sie kein zusätzliches clusterfähiges Dateisystem für den gemeinsamen Zugriff mehrerer Hosts benötigen.

Performance-Engpässe ergeben sich in virtualisierten Umgebungen durch das parallele Zugreifen mehrerer Gäste mit unterschiedlichen Zugriffsmustern, wobei Volume-Größen, RAID-Konfigurationen und die richtige Lastverteilung eine Rolle spielen.

Nadelöhr Massenspeicher

Bei der Platzaufteilung gilt: Zu viele kleine Volumes für einzelne Vdisks erhöhen den Verwaltungsaufwand und können zu hohem Verschnitt führen; zu große mit vielen Vdisks können Performance-Engpässe auslösen. Leistungskiller sind die konkurrierenden Gastzugriffe auf ein RAID-Set und die hohe Zahl sogenannter SCSI-Reservierungen bei Zugriffen auf ein VMFS-Volume durch mehrere Hosts. Letztere benutzt der VMFS-Manager zum Sperren des Dateisystems, wenn er Metadaten ändert.



VMware Converter überträgt physische und virtuelle Maschinen und passt die Controller-Treiber im Gast an (Abb. 4).

Eine gute Ausgangsgröße sind Volumes von etwa 200 bis 500 GByte, mit jeweils fünf bis zehn virtuellen Platten. Bei geringer Auslastung dürfen es deutlich mehr Vdisks pro Volume sein. Erreichen die Gäste die Leistungsanforderungen nicht mehr, müssen Vdisks auf andere Volumes umziehen.

In kleineren Umgebungen genügen oft zwei bis drei Volumes auf einem einzigen RAID-Set. Je nach physischer Plattenanzahl ist eine Aufteilung in mehrere RAID-Sets nicht immer sinnvoll, da erst eine größere Anzahl Spindeln optimale Leistung liefert. Die Aufteilung eines RAID-Sets in mehrere Volumes kann dagegen nützlich sein, beispielsweise um Produktiv- und Testumgebung zu trennen oder die Last über mehrere Zugriffspfade zu verteilen.

Leistungshungrige Gäste wie große Datenbanken oder Exchange Server erfordern eine genauere Planung des RAID-Levels. RAID 5 bietet optimale Platzausnutzung, RAID 10 dagegen optimale Leistung. RAID-Sets mit unterschiedlichen RAID-Leveln auf unterschiedlich schnellen Festplatten können Vdisks je nach Leistungsanforderung aufnehmen. Ein guter Mix aus gering bis stark belasteten Vdisks optimiert die Zugriffe auf ein Volume. Virtuelle Platten mit extrem hohem Leistungsbedarf sollten ein separates RAID-Set bekommen.

Ein klassischer Fehler liegt in der falschen Anordnung der Vdisks eines Gastsystems auf dem physischen Speicher. So kann ein virtueller Datenbank-Server korrekt mit getrennten Vdisks für System, Datenbank und Transaktionslogs arbeiten. Diese Trennung nützt aber nichts, wenn alle Vdisks auf dem gleichen Volume liegen. Solche Fehler führen vor allem in hochlastigen Umgebungen zu Performance-Einbrüchen.

Für weiteres Kopfzerbrechen sorgt die Lastverteilung. Ein Host benutzt immer denselben Zugriffspfad und dieselbe Queue für ein bestimmtes Volume mit allen dort liegenden Vdisks. Eine Lastverteilung lässt sich nur mit mehreren Volumes erreichen. Bei einem einzigen Volume dienen zwei im Host eingebaute HBAs ausschließlich der Redundanz – einer liegt immer brach. Für eine flexiblere Lastverteilung unterstützt ESX Server seit Version 3.5 Round-Robin Load Balancing, allerdings noch als experimentelle Option.

Ein weiteres Planungskriterium sind Spiegelungen. Will man die Kosten des doppelt vorzuhaltenden Plattenspeichers nicht unnötig in die Höhe treiben, sollte man nur die Volumes spiegeln, auf denen die VMs mit höchstem Service-Level liegen. Unwichtigere Gäste residieren dann auf preiswerterem Speicher.

Nicht zuletzt ist zu beachten, dass das Zoning beziehungsweise LUN-Masking im SAN nicht mehr einzelne Systeme, sondern ganze Hosts mit vielen Gästen betrifft. Einige Virtualisierer bieten N_Port (Node-Port) ID Virtualization (NPIV), was die Zuweisung eines expliziten World Wide Port Name (WWPN) zu einzelnen Gästen ermöglicht.

Planungsfehler beim Speicher lassen sich nachträglich durch die zu bewegenden Datenmengen nur mit langen Ausfallzeiten korrigieren. Hier setzt die Funktion Storage VMotion von VMware Infrastructure 3.5 an. Sie migriert VMs mitsamt allen Vdisks unterbrechungsfrei von einem Speicherort zum anderen, etwa wenn ein Volume voll ist oder das RAID-Set an seine Leistungsgrenze gerät. Dazu

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

benutzt es Snapshots, die während der Migration die Zugriffe der Gäste in sogenannte Redo-Logs (Deltas) puffern.

Arten virtueller Platten

Nach der Planung des physischen Speichers muss sich der Admin für einen Typ der Vdisk entscheiden. Zur Auswahl stehen Zuwachsplatten und vorreservierte Platten.

Zuwachsplatten enthalten nur die Sektoren, die der Gast wirklich belegt. Die Containerdatei wächst nach Bedarf und nutzt den vorhandenen physischen Platz optimal aus. Zuwachsplatten verlangen eine ständige Überwachung des physischen Speicherplatzes. Geht er zur Neige, stürzen im schlimmsten Fall die Gastsysteme ab. Zudem leidet die Performance mit der Zeit, weil die Containerdateien auf die Dauer fragmentieren und das blockweise Wachstum der Dateien dem Host zusätzlichen Verwaltungsaufwand beschert.

Zuwachsplatten verringern ihre Größe nicht mehr, selbst wenn der Gast sein Dateisystem aufräumt. Die Virtualisierer bieten dafür Shrink- beziehungsweise Compact-Funktionen, die unbelegten Platz in Vdisks wieder entfernen.

Das Gegenstück sind vorreservierte Vdisks, die bereits beim Erstellen den gesamten zugewiesenen Platz physisch belegen. Es entstehen sofort große unfragmentierte Containerdateien. Der Platz ist sicher reserviert und die Performance ist bei I/O-lastigen Gästen besser. Dafür liegt ungenutzter Platz brach, der sich bei vielen VMs zu Terabytes summieren kann.

Grundsätzlich empfiehlt es sich, in Testumgebung Zuwachsplatten und in leistungshungrigen Umgebungen vorreservierte Platten zu verwenden. In kleineren Produktivumgebungen mit wenig verfügbarem Platz und moderatem Leistungsbedarf kann der Einsatz von Zuwachsplatten viel Platz sparen. Vorhandene Vdisks lassen sich bei manchen Virtualisierern nachträglich per Kommandozeile umwandeln.

Alle Virtualisierer legen Vdisks automatisch als monolithische Dateien an. Bei Bedarf lassen sich die Dateien aber in Segmente, meist in 2-GByte-Einheiten, unterteilen. Damit kann die Vdisk auch auf einem alten FAT-Dateisystem residieren oder auf DVD umziehen.

Direkter Durchgriff ohne Container

Unabhängig vom Plattentyp sollten Gastsysteme immer mit getrennten Vdisks für System, Daten und gegebenenfalls Swapfile oder Swap-Partitionen ausgestattet sein. Dadurch lassen sie sich flexibler klonen, sichern und auf den physischen Datenträgern verteilen.

In Ausnahmefällen erlauben die Virtualisierer per Raw Device Mapping (RDM), bei Microsoft als Passthru bezeichnet, den Durchgriff eines Gastes direkt auf den Datenträger, ohne Umweg über eine Containerdatei. Das ermöglicht Dual-Boot-Konfigurationen zwischen Hardware und VM oder den Wechsel eines Volumes zwischen VMs und physischen Servern, etwa bei Clustern, deren Quorums- und Datenspeicher auf gemeinsamen Volumes liegen. Zudem lassen sich per RDM native Features des Storage-Gerätes auch in VMs nutzen, etwa SAN-Snapshots oder spezielle Sicherungsoptionen.

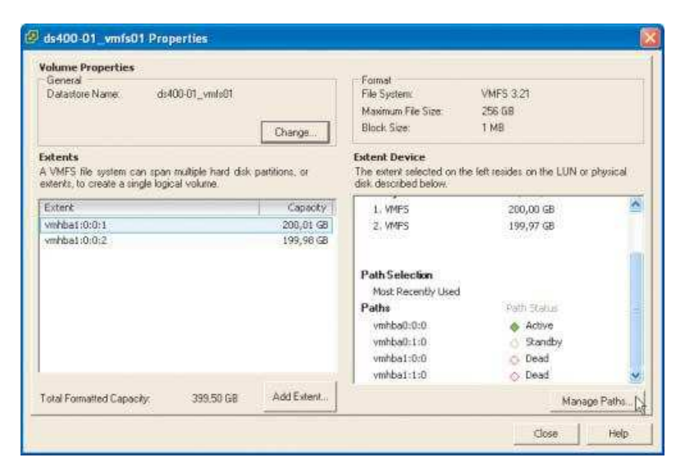
Eine recht unbekannte Option der direkten Speicheranbindung ist die Installation eines Software-iSCSI-Initiators im Gast und der Zugriff auf Volumes über virtuelle Netzwerkkarten. Zumindest die Boot-Partition des Gastsystems muss aber auf einer Vdisk liegen, es sei denn, man richtet sich – etwa mit Open-iSCSI – eine iSCSI-Boot-Konfiguration über die virtuelle Netzwerkkarte ein [2]. Auch Microsofts Software-Initiator unterstützt seit der Version 2.06 das Booten per iSCSI. Diese Methode ist völlig unabhängig vom Virtualisierer.

Die bisher erörterten Kriterien, wie physischer Speicherort und Typ der Containerdatei, beschreiben die Sicht des Host auf die virtuellen Platten. Die Sicht eines Gastes auf die Vdisks prägt ausschließlich der emulierte Controller, den der Virtualisierungslayer vorgaukelt.

VMware emuliert entweder einen SCSI-Controller von LSILogic oder BusLogic. Alle VMware-Produkte bis auf ESX Server unterstützen virtuelle IDE-Platten. Microsoft emuliert einen Adaptec-SCSI-Controller oder IDE-Adapter. Virtual PC unterstützt keine SCSI-Platten und Hyper-V kann Gäste nur von virtuellen IDE-Platten booten. XEN bietet ebenfalls virtuelle SCSI- und IDE-Platten.

Grundsätzlich verursachen IDE-Platten weniger Schwierigkeiten, da jedes Gastsystem generische Treiber mitbringt. Virtuelles SCSI kann dagegen aufgrund seiner Architektur mehr als vier virtuelle Platten anbieten.

Entscheidend im Gast ist der zum emulierten Controller passende Treiber. Er ist wichtig bei der Installation des



ESX Server integriert wichtige Funktionen wie Multipathing im SAN für die Speicheranbindung (Abb. 3).

Dateien virtueller Platten

Containerdateien bei Microsoft	
Vdisk	**.vhd*
Undo-Disks Virtual Server/PC	**.vud* (entstehen beim Einschalten von Rückgängig-Datenträgern automatisch)
Differencing Disks Virtual Server/PC	**.vhd* (manuell zu erzeugen und einzubinden, Kaskadierung manuell möglich)
Snaphots Hyper-V	**.avhd* (im Snapshot-Ordner, kaskadierend für jeden Snapshot)
Containerdateien bei VMware	
Vdisk	**.vmdk*
undoable Disks	**.vmdk.REDO_a01736* (mit Zufallsnummer zur Unterscheidung)
Snapshots	**-000001.vmdk* (kaskadierend mit laufender Nummer für jeden Snapshot)
weitere Dateien	
Bei Snaphots laufender Gäste (Save State) entstehen zusätzliche Dateien mit RAM-Inhalt und Systemstatus der VM, die nichts mit der Vdisk zu tun haben:	
Microsoft	**.bin und *.vsv*
VMware	**.vmem und *.vmsn*

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Gastsystems und bei der Übertragung von VMs zwischen unterschiedlichen Virtualisierern. Beim Verschieben von physischen auf virtuelle Rechner (P2V, physical to virtual) muss man den Treiber ebenfalls anpassen. Bootet eine VM ohne den passenden Controller-Treiber, führt das – unter Windows – unvermeidlich zum Bluescreen.

Mittlerweile übernehmen Konverter bei der Virtualisierung physischer Rechner (P2V) und beim Übertragen von VMs (V2V) die Anpassung der Controller-Treiber. Zu ihnen gehören der frei verfügbare VMware Converter, der in Workstation und Virtual Center bereits integriert ist (www.vmware.com/products/converter), und Acronis Universal Restore (www.acronis.de/enterprise/products/ATIES/universal-restore.html).

Eine Alternative zu Konvertern bildet das manuelle Vorinstallieren des Treibers vor dem Übertragen des Systems. Nähere Informationen zu den virtuellen Controller-Typen und Treibern finden sich unter www.vmaschinen.de/cgi-bin/vmware.cgi?scsi. Die meisten Virtualisierer liefern leistungsoptimierte Treiber, die nachträglich im Gastsystem installiert werden, etwa über die VMware Tools oder MS Virtual Machine Additions.

Besondere Funktionen

Neben ihrer Datenträger-Unabhängigkeit bieten Vdisks weitere, ganz spezifische Vorteile: Bei einem Snapshot leitet der Virtualisierer Schreibzugriffe des Gastes in eine separate Datei, das sogenannte Redo-Log oder Delta um. Dadurch bleibt der Inhalt der Vdisk unangetastet. Änderungen lassen sich jederzeit verwerfen oder übernehmen.

Redo-Logs sind zusätzliche Containerdateien, die nur veränderte Sektoren einer Vdisk enthalten. Mehrere Redo-Logs lassen sich kaskadieren (multiple Snaphots), um unterschiedliche Zustände eines Gastes zu sichern. Microsoft nannte seine Redo-Logs bisher Rückgängig-Datenträger, erst seit Hyper-V existiert dort der Begriff Snapshot.

Neben dem Verwerfen von Fehlern ermöglichen Redo-Logs das schnelle Erzeugen von Klonen (linked Clones). Dabei verwenden mehrere VMs über Deltas die gleiche virtuelle Platte, was viel Platz spart und wenig Zeit beim Klonen kostet.

Eine weiterer Einsatzzweck von Snapshots sind Hot-Backups des Gastsystems, also Sicherungen im laufenden Betrieb. Da ein Redo-Log die Vdisk von Schreibzugriffen des Gastes abkoppelt, lässt sich die Vdisk im laufenden Betrieb sichern. Damit arbeitet beispielsweise VMware Consolidated Backup. In Kombination mit gemeinsam genutztem Speicher ermöglicht es die LAN-freie Sicherung von Gästen im SAN über einen Backup-Proxy. Solche Optionen virtueller Platten ergänzen oder ersetzen herkömmliche LAN-Backups mit Agenten in den Gastsystemen. (sun)

SVEN AHNERT

arbeitet als freier IT-Berater und Fachautor. Er betreibt die Webseite www.vmaschinen.de und ist Autor des Buches „Virtuelle Maschinen mit VMware und Microsoft“.

Literatur

[1] Fred Hantelmann; Virtualisierung; Halbrund; Microsofts Virtualisierer Hyper V; *iX* 8/2008, S. 66

[2] Michael Riepe; Storage; Verlängerte Wurzel; Booten aus dem Speichernetz; *iX* 9/2004, S. 121





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Zertifikatskontrolle mit OCSP-Proxies

Flink geprüft

Daniel Fischer, Jürgen Key, Peter Steiert

Zur digitalen Signatur gehört untrennbar ihre Prüfung. Ein Aspekt dabei ist die Gültigkeit des benutzten Zertifikats, deren Kontrolle sich mit einem Proxy vereinfachen lässt.

Digitale Signaturen gewinnen in der Geschäftswelt an Bedeutung. Einige typische Anwendungsfälle sind die elektronische Rechnung, das Elektronische Gerichts- und Verwaltungspostfach (EGVP) und der elektronische Rechtsverkehr in Deutschland (ERV-D). Aber nicht nur Unternehmen, sondern auch Privatpersonen werden digitale Signaturen immer häufiger einsetzen, zum Beispiel beim elektronischen Einkommensnachweis (Elena) und der elektronischen Steuererklärung (Elster).

Eine qualifizierte elektronische Signatur ermöglicht – analog zur herkömmlichen Unterschrift auf Papierdokumenten – das „Unterzeichnen“ elektronischer Daten, beispielsweise einer Datei oder einer Mail. Gesetzlich ist sie der eigenhändigen Unterschrift hinsichtlich des Beweiswerts gleichgestellt. Außer der qualifizierten Signatur kennt das Signaturgesetz (SigG) die fortgeschrittene und die einfache elektronische Signatur. Sie bieten weniger Rechtssicherheit als die qualifizierte, sind allerdings leichter zu erstellen und preiswerter. Die fortgeschrittene und die qualifizierte Signatur geben Auskunft über die Identität ihres Erstellers. Außerdem erlauben sie, die Unversehrtheit (Integrität) der signierten Daten zu prüfen.

Technisch betrachtet entsteht eine fortgeschrittene oder qualifizierte Signatur, indem der Unterschreibende über die zu signierenden Daten einen Hash-Wert (Prüfsumme) bildet, den er mit seinem privaten Schlüssel verschlüsselt. Zur Verschlüsselung dienen in der Regel digitale Zertifikate wie X.509-Zertifikate. Die Prüfung einer elektronischen Signatur umfasst die Kontrolle der Zertifikatgültigkeit und der Datenintegrität.

Zertifikate müssen noch gelten

Besondere Anforderungen stellt vor allem der erste Teilprozess (auf eine detaillierte Betrachtung der Integritätsprüfung wird im Folgenden verzichtet). Um die Authentizität des Signaturerstellers zu überprüfen, muss die Korrektheit und Gültigkeit seines privaten Schlüssels verifiziert werden. Bei der Verwendung digitaler Zertifikate bezieht sich diese Kontrolle hierzulande auf den Sachverhalt, ob das zur Generierung der Signatur benutzte Zertifikat zum Erstellungszeitpunkt gültig (und korrekt) war.

Zur Vereinfachung sei angenommen, dass alle notwendigen Prüfungen vor und während des Einsatzes digitaler Zertifikate korrekt stattgefunden haben, etwa die Registrierung durch die Registration Authority (RA) oder die Ausstellung durch eine vertrauenswürdige Certificate Authority (CA). Der erste Schritt zur Überprüfung der Gültigkeit eines Zertifikats ist die Kontrolle seiner Lebensdauer. Diese Beschränkung der Laufzeit „ab Werk“ soll Änderungen technischer und organisatorischer Art begegnen. Die Lebensdauer ist im Zertifikat enthalten und lässt sich somit relativ einfach kontrollieren. War es bei der Erstellung der Signatur bereits abgelaufen, steht die Identität des Signaturerstellers nicht mit Sicherheit fest.

Komplizierter wird es jedoch, wenn das Zertifikat vor der voreingestellten Gültigkeitsdauer abläuft. Beispielsweise kann eine Firma ihrem Prokuristen bei der Entlassung sein Zertifikat entziehen, damit er keine Geschäfte mehr im Namen der Firma tätigen kann. Ein weiteres Beispiel tauchte vor wenigen Wochen auf, als eine Sicherheitslücke in der OpenSSL-Bibliothek verschiedener Debian-Distributionen die mit ihr erzeugten Zertifikate angreifbar machte. Daraufhin musste die Nutzung solcher Zertifikate unterbunden werden. Ein solches außerplanmäßiges Beenden der Gültigkeit digitaler Zertifikate heißt „Sperren“.

Wie kann nun der Empfänger elektronisch signierter Daten erfahren, ob das verwendete Zertifikat noch gilt? Da es in der Vergangenheit ausgestellt und dem Anwender übergeben wurde, lässt sich nicht nachträglich das Ende seiner Gültigkeit vorverlegen. Aktuelle Informationen zum Status eines Zertifikats kommen in der Regel vom Zertifizierungsdiensteanbieter, dem Betreiber der CA. Ihm stehen zwei Verfahren zur Verfügung, Sperrinformationen bereitzustellen.

Zwei Methoden der Prüfung

Variante eins sind sogenannte Sperrlisten (Certificate Revocation Lists, CRLs [a]). Sie enthalten Seriennummern gesperrter Zertifikate und die Sperrgründe (Reason Codes). Es ist möglich, eine URL für den Bezug der Liste durch eine standardisierte Erweiterung direkt im Zertifikat zu speichern. Der Empfänger der signierten Daten muss somit die aktuelle CRL der ausstellenden CA herunterladen und prüfen, ob sie die Seriennummer des empfangenen Zertifikats enthält. Fehlt sie, gilt das Zertifikat. Dieses Verfahren birgt jedoch mehrere Nachteile:

– CRLs können sehr groß sein.
– Sie müssen vollständig auf dem Client zur Verfügung stehen, der sie erst nach dem

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

kompletten Herunterladen prüfen kann. Gerade auf mobilen Geräten ist die Ladezeit lästig. – Zwischen in der Regel zu festen Terminen erfolgenden Veröffentlichungen von CRLs ist keine zuverlässige Prüfung möglich.

Eine zweite Variante, Informationen über Zertifikatssperrungen zur Verfügung zu stellen, bietet das Online Certificate Status Protocol (OCSP, [b]), das Positivauskünfte vom Aussteller des Zertifikats liefert. Der Anwender fragt einen sogenannten OCSP-Responder nach der Gültigkeit des Zertifikats. Dieser antwortet mit dem Status „good“ (gültig), „revoked“ (gesperrt) oder „unknown“ (keine Informationen vorhanden). Benutzt der OCSP-Responder die aktuelle Datenbasis der CA, kann er – anders als CRLs – nahezu in Echtzeit über die Gültigkeit der Zertifikate informieren. Außerdem liefert er nur Statusinformationen zu angefragten Zertifikaten, was Zeit spart, und OCSP entlarvt gefälschte Zertifikate – vorausgesetzt, der Responder liefert nur bei existierenden, nicht gesperrten Zertifikaten „good“ zurück. Sowohl CRLs als auch OCSP informieren über den genauen Zeitpunkt der Sperrung.

Anwender, die mit vielen Zertifikaten von unterschiedlichen CAs konfrontiert sind, stehen vor der Aufgabe, jedes von ihnen auf seine Gültigkeit zu testen. Dazu sind je nach CA CRLs zu holen oder OCSP-Requests zu generieren und deren Statusinformationen auszuwerten. Besonders in der Kommunikation zwischen Unternehmen entwickelt sich daraus eine komplexe Aufgabe. Die Bezugsstellen für CRLs und OCSP-Server können in Zertifikaten vermerkt sein – müssen aber nicht. Adressen von OCSP-Diensten muss man für jeden Provider einzeln pflegen. Diese Aufgaben kosten noch mehr Zeit, wenn mehrere Anwendungen digital signierte Daten verarbeiten. Neben dem Aufwand für die Pflege dieser Konfigurationen wächst die Anfälligkeit für Fehler in ihnen.

Der Proxy maskiert OCSP und CRL

Ein OCSP-Proxy kann den Aufwand reduzieren und die Konfiguration vereinfachen: Er beantwortet allen Anwendungen die Frage nach der Gültigkeit digitaler Zertifikate, indem er die Anfragen an die in seiner Konfiguration festgelegten zuständigen OCSP-Responder sendet. Die Antworten sammelt er ein und übermittelt sie an die Anwendungen. Ändert sich die Adresse eines Responders oder kommen neue hinzu, muss man nur noch die Proxy-Konfiguration anpassen – in den Anwendungen sind keine Änderungen erforderlich. Neue Programme benötigen nur einmalig die Adresse des Proxy und haben sofort Zugriff auf einen OCSP-Responder.

Keine Anwendung braucht mehr mit CRLs umzugehen, denn sie stellt Anfragen für jedes Zertifikat nur noch als OCSP-Request an den Proxy. Publiziert der Aussteller lediglich CRLs zur Gültigkeitsprüfung, holt der Proxy diese Listen, analysiert sie und erzeugt daraus eine OCSP-Antwort, die er an die Anwendung sendet. Somit können Entwickler Code zur Behandlung von CRLs entfernen und ihn sich in neuen Anwendungen sparen. Das Ergebnis sind kleinere, weniger fehleranfällige Programme und unter Umständen ein leistungsfähigeres Gesamtsystem.

Die Firma NetSys.IT hat einen OCSP-Proxy geschaffen, den man in bestehende Infrastrukturen integrieren kann. Nach Abschluss des zurzeit laufenden nichtöffentlichen Betatests will sie ihn als Open-Source-Projekt freigeben. Der in Java als Servlet geschriebene Proxy kann in jedem Container laufen, der die Servlet-API ab Version 2.2 unterstützt. Die Arbeit mit digitalen Zertifikaten/Signaturen übernimmt der Cryptoprovider von Bouncy Castle [c]. Dieses Programm dient als reiner Proxy für OCSP und als Fassade für CRLs. Allerdings lädt es CRLs von den CAs nicht erst bei einer Anfrage. Vielmehr holt der Proxy die Listen regelmäßig selbsttätig und speichert sie in einer relationalen Datenbank. Aus ihr generiert er die OCSP-Responses. So können auch Organisationen, die derzeit keinen eigenen OCSP-Dienst bereitstellen, diese Funktion einfach anbieten. Das zyklische Laden der CRLs berücksichtigt den in ihnen vermerkten voraussichtlichen nächsten Aktualisierungszeitpunkt.

Ein solcher OCSP-Proxy als einziger Zugangspunkt bedeutet pessimistisch betrachtet gleichzeitig ein Ausfallrisiko. Dies ist allerdings nicht unausweichlich, da OCSP als zustandsloses Protokoll Load Balancing und Hochverfügbarkeit relativ einfach ermöglicht. Beides sollte auf jeden Fall abhängig von der anvisierten Nutzerzahl für den Proxy eingerichtet sein, da die Anwender ihn nicht akzeptieren, wenn er für die Beantwortung der OCSP-Anfragen signifikant länger braucht als die CAs. Allerdings kann der Proxy prinzipbedingt nicht schneller antworten, wenn er auf OCSP-Provider zurückgreift. Stammen die nötigen Informationen aus CRLs, bietet er jedoch einen Geschwindigkeitsvorteil. In diesem Fall tritt das Lesen aus der Datenbank an die Stelle des Ladens der gesamten Liste. Damit bestimmt die Leistung der Datenbank die Antwortzeit des Proxy.

Schließlich ist ein OCSP-Proxy nicht mit einer Implementierung des Server-based Certificate Validation Protocol SCVP [d] zu verwechseln. SCVP geht weit über OCSP hinaus, da es die Prüfung von Zertifikaten komplett übernimmt. Das umfasst auch den Aufbau der Zertifikatskette und deren Prüfung. Damit befreit SCVP die Anwendungen von der Validierung einer Signatur. Es bietet hierzu einige vielversprechende neue Ansätze und Erweiterungen. Allerdings muss dieser neue Standard seine Einsatzreife erst noch unter Beweis stellen. Bis dahin stellt OCSP eine sehr gute Lösung dar. (ck)

JÜRGEN KEY

ist Partner der Firma NetSys.IT. Als Senior-Softwaredesigner beschäftigt er sich mit allen Aspekten der Objektorientierung.

PETER STEIERT

ist Partner der Firma NetSys.IT. Als Senior-IT-Security-Spezialist beschäftigt er sich mit allen Aspekten der IT-Sicherheit.

DANIEL FISCHER

ist wissenschaftlicher Mitarbeiter am Lehrstuhl „Informations- und Wissensmanagement“ der TU Ilmenau und Geschäftsführer der Firma NetSys.IT.



[a]	RFC zu Certificate Revocation Lists	http://tools.ietf.org/html/rfc3280
[b]	RFC zu OCSP	http://tools.ietf.org/html/rfc2560
[c]	Bouncy Castle	www.bouncycastle.org
[d]	RFC zu SVCP	http://tools.ietf.org/html/rfc5055

Literatur

[1] Luigi Lo Iacono, Sibylle Müller, Michael Schneider; Digitale Signaturen; Modelle zur Gültigkeitsprüfung von Zertifikaten; Gültige Pfade; *iX* 6/06, S. 126





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Mehr Datensicherheit mit Oracle Data Guard

Graue Eminenz

Martin Bach

Datenbanken wachsen stetig, und fallende Speicherpreise ermutigen Softwarehersteller nicht zum Schreiben von Archivierungslösungen. Die daraus resultierenden großen Datenmengen bedeuten zwangsläufig lange Wiederherstellungszeiten im Fehlerfall. Standby-Datenbanken versprechen Abhilfe.

Oracles Data Guard Option erlaubt es, eine Standby- als Kopie der Produktionsdatenbank zu betreiben. Alle Transaktionen der Produktionsdatenbank führt sie anhand archivierter Online Redo Logs nach. Zu den Vorzügen einer solchen Konfiguration zählen Verfügbarkeit, Datensicherheit, Disaster Recovery.

Für das Verständnis von Data Guard ist ein wenig Hintergrundwissen über Oracle nötig. Wie alle modernen RDBMS verwendet es einen Teil des Hauptspeichers als Cache für häufig benutzte Datensätze. Die kleinste Einheit darin ist der Block, der in den meisten Fällen 8 KByte groß ist. Ändert sich ein Block durch eine Transaktion, schreibt ihn der dafür zuständige Database Writer (*DBWR*) in der Regel nicht sofort auf die Platte, denn das wäre zu ineffizient. Stattdessen sammelt er eine Reihe modifizierter Blöcke und schreibt sie in einem Rutsch.

Da eine der ACID-Forderungen (Atomicity, Consistency, Isolation, Durability) an Transaktionen die Beständigkeit der Daten nach einem *commit* ist, muss der Server die Transaktionen im Fehlerfall wiederherstellen können. Dazu dienen vom Hintergrundprozess Log Writer (*LGWR*) geschriebene Online Redo Logs, die Veränderungen der Daten protokollieren und die geforderte Dauerhaftigkeit garantieren. Fällt der Strom aus, kann der Server die im Hauptspeicher veränderten Blöcke nicht mehr auf die Platte schreiben, die Datenbank ist inkonsistent. Beim folgenden Neustart verwendet er automatisch die Informationen aus den Online Redo Logs, um mittels *commit*-Befehl abgeschlossene Transaktionen wiederherzustellen – daher „Redo“ Log.

Online Redo Logs fasst Oracle in Gruppen zusammen, was die Datensicherheit erhöht. Diese Gruppen beschreibt es zirkulär: Sind alle Redo-Log-Dateien der aktuellen Gruppe vollgeschrieben, schaltet Oracle zur nächsten um (Log Switch). Ist es bei der letzten angelangt, beginnt es wieder bei der ersten. Für die Wiederherstellung der Datenbank sind diese Online Redo Logs von großer Bedeutung, weshalb Oracle bei jedem Log Switch die zuletzt verwendete Log-Datei archiviert und sie an einen anderen Ort auf dem Server kopiert.

Aktualisieren jetzt oder später

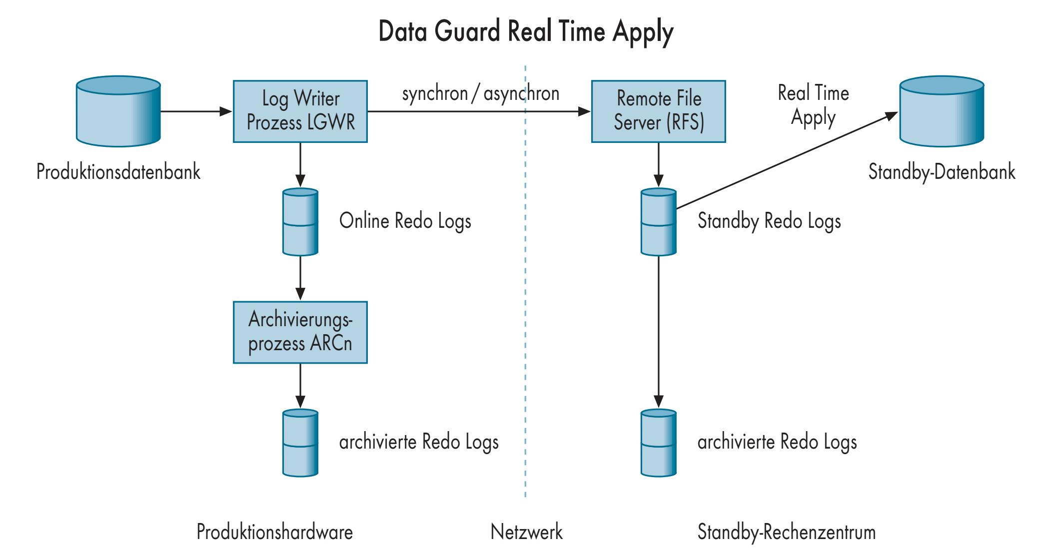
In einer typischen Konfiguration von Data Guard schreibt *LGWR* sowohl in die lokalen Online Redo Logs als auch über das Netz in sogenannte Standby Redo Logs der Standby-Datenbank. Sind sie ebenfalls gefüllt, archiviert der Server sie lokal; danach führt er automatisch ein Recovery der Standby-Datenbank durch. Das stellt die Gleichartigkeit der Daten zwischen Produktions- und Standby-Datenbank sicher. Besteht aus technischen Gründen, zum Beispiel aufgrund einer Netzwerkstörung, keine Verbindung zwischen Produktions- und Standby-Datenbank, fordert Data Guard automatisch die fehlenden Online Redo Logs von der Produktionsinstanz an, nachdem der Fehler behoben ist. Diese gesamte Prozedur taucht erstmals als „Managed Recovery“ in Oracle 9.0.1 auf. Mit Oracle 10.1 kam „Real Time Apply“ (siehe Abbildung 1). Es ermöglicht, Redo-Information direkt nach ihrem Eintreffen in der Standby-Datenbank anzuwenden; ein Warten auf den Log Switch der Standby Redo Logs entfällt.

Etwas Ähnliches wie Managed Recovery könnte auch

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ein Datenbankadministrator implementieren. Allerdings erfordert dies Programmieraufwand, und er müsste die Fehlerbehebung sowie das Anfordern fehlender Redo Logs selbst erledigen. Weiterführende Fähigkeiten wie der lesende Zugriff auf die Standby-Datenbank ist mit einer solchen Heimwerkerlösung nicht ohne Weiteres möglich.

Außer der eben beschriebenen Physical Standby-Datenbank gibt es eine logische. Anders als die erste, die sich permanent im Recovery-Modus befindet und daher in der Regel nicht für Benutzer zur Verfügung steht, ist die logische Standby-Datenbank allgemein zugänglich und kann zum Beispiel Reporting-Aufgaben übernehmen. Ihr Inhalt kann jedoch von der Produktionsdatenbank abweichen. Beim Erstellen bekommt die logische Standby-Datenbank eine eigene Datenbank-ID zugewiesen, was ein Recovery mittels archivierter Logs von der Produktionsdatenbank ausschließt.



Oracles Real Time Apply führt alle Änderungen der Produktionsdatenbank sofort auf der Standby-Kopie durch (Abb. 1).

Logischer statt physischer Standby

Data Guard transformiert stattdessen die Daten der Redo Logs mit Log Miner in SQL-Anweisungen, die es auf die Datenbank anwendet. Die Verwendbarkeit einer logischen Standby-Datenbank für den Umstieg auf eine andere Server-Version („Rolling Upgrade“, siehe *iX*-Link) ist nach Ansicht des Autors ihr größter Pluspunkt. Außerdem können Entwickler Datenbankobjekte in eigenen Schemata anlegen, die aus organisatorischen Gründen auf der Produktionsdatenbank nicht erlaubt wären.

Trotz dieser Vorzüge logischer Standby-Datenbanken scheinen sie weniger verbreitet zu sein als die physische, was sicherlich an einigen Einschränkungen etwa bei den unterstützten Datentypen liegt. Dieses Ungleichgewicht könnte sich mit Oracle 11 ändern, da sich zum einen die Menge der unterstützten Datentypen von Release zu Release vergrößert hat. Zum anderen lässt sich eine physische Standby-Datenbank mit einem einzigen Kommando für die Dauer der Migration in eine logische konvertieren, was den Umstieg stark vereinfacht.

Eine physische Standby-Datenbank kann man zwar für lesenden Zugriff öffnen, in dieser Zeit übernimmt sie aber keine Änderungen von der Produktionsdatenbank. Früher konnte dies zu Schwierigkeiten führen, wenn der DBA den Lesezugriff wieder abschaltete und sie damit in den Managed Recovery Modus versetzte: In diesem Moment fordert sie eine Flut von Logfiles von der Produktionsdatenbank an, die sie anwenden muss, um zu ihr aufzuschließen. Je nachdem wie geschäftig die Produktionsvariante war, konnte dies lange dauern. Das mit Oracle 11 eingeführte „Active Data Guard“ erlaubt es nun endlich, die Standby-Datenbank für den lesenden Zugriff zu öffnen und gleichzeitig die Änderungen der Produktion einzuarbeiten.

Als dritte Standby-Variante kam mit Oracle 11 die sogenannte Snapshot-Datenbank hinzu. Das ist eine modifizierte physische Standby-Datenbank. Zwei Vorzüge zeichnen sie nach Erachten des Autors aus: Zum einen können Anwender lesend und schreibend darauf zugreifen, zum anderen empfängt sie zwar Logs von der Produktion, wendet sie aber nicht an. Konvertiert der DBA die Snapshot- wieder zur physischen Standby-Datenbank, verwirft sie alle Änderungen und wendet die zwischenzeitlich gesammelten Logs an. Ein solcher Snapshot eignet sich hervorragend für den Test von Ad-hoc-Änderungen an einer aktuellen Kopie der Produktion und bringt dennoch die Vorzüge einer Standby-Datenbank. In Oracle 10 ist dies zwar ebenfalls möglich, erfordert aber dort mehr manuellen Aufwand: Nach dem Setzen eines garantierten Restore Point muss der DBA die Standby-Datenbank wie im Ernstfall aktivieren. Nach dem Ende der Tests versetzt er sie per Flashback [1] wieder zurück in die Standby-Rolle, die Redo Logs anfordert und anwendet.

Data Guard bietet die Sicherheitsstufen „Maximum Performance“, „Maximum Availability“ und „Maximum Protection“. Die erste ist die Standardeinstellung und erlaubt den besten Kompromiss zwischen Sicherheit und Performance. Redo-Informationen fließen asynchron von der Produktions- zur Standby-Datenbank, ohne dass der Absender auf eine Bestätigung wartet.

Hohe Sicherheit hat ihren Preis

„Maximum protection“ ist die höchste Sicherheitsstufe und garantiert Datenerhalt, sollte die Produktionsdatenbank nach einem schweren Fehler nicht mehr verfügbar sein.

iX-TRACT

- Oracles Data Guard ermöglicht den Betrieb einer Standby-Datenbank mit identischem Bestand wie das Produktivsystem.
- Diese Konfiguration erleichtert das schnelle Umschalten bei einem Hardwaredefekt und vereinfacht die Migration auf eine neue Server-Version.
- Mit dem Real Application Cluster desselben Herstellers lassen sich ähnliche Anforderungen nur bei höheren Hardwarekosten erfüllen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Dieser Modus benötigt Redo Logs auf der Standby-Datenbank und überträgt die Redo-Informationen synchron. Für die Höchstsicherheit muss man jedoch einen Preis zahlen: Scheitert eine Transaktion beim Senden der Redo-Informationen an die Standby-Datenbank und deren Redo-Logs, fährt die Produktionsdatenbank kontrolliert herunter. Temporäre Netzprobleme können sich so unliebsam bemerkbar machen. „Maximum Availability“ liegt zwischen den beiden anderen Konfigurationen.

In Data Guard können Datenbanken auf zwei Arten ihre Rollen tauschen: per Umschalten (Switchover) und Übernahme im Fehlerfall (Failover). Ersteres findet in der Regel für Wartungsarbeiten auf dem Produktionsserver statt und ist im Voraus geplant. Beim Failover ist es aus technischen Gründen (zum Beispiel Hardwaredefekt) nicht möglich, die Produktionsdatenbank weiter zu betreiben. Der Vorteil einer Standby-Datenbank liegt in dieser Situation darin, dass sie ohne das langwierige Einspielen einer Sicherung vom Band sofort loslegen kann. Datenverlust kann beim Umschalten nicht auftreten, wohl aber bei einem Failover.

Bis Oracle 9i musste man die ehemalige Produktionsdatenbank nach einem Failover komplett neu erstellen, was ein Restore und Recovery einer Sicherung erforderte. Release 10 brachte große Verbesserungen in dieser Situation. Zum einen bietet Real Time Apply auch bei Maximum Performance relativ hohe Datensicherheit, da Informationen gleichzeitig in die Online Redo Logs der Produktions- und Standby-Datenbanken geschrieben werden. Zum anderen kann Flashback die ehemalige Produktionsdatenbank nach Korrektur des Hardwaredefekts in eine Standby-Datenbank überführen. Laut Dokumentation sind dazu 14 Punkte abzuarbeiten. Der mit 9.0.1 eingeführte „Data Guard Broker“ erledigt diese Aufgabe per *reinstate database*.

Data Guard Broker soll es weniger erfahrenen Operatoren ermöglichen, Rollenwechsel problemlos durchzuführen. Die Erfahrung zeigt, dass sein Einsatz den gesamten Prozess wesentlich vereinfacht: Ein einziges Kommando kann den Rollenwechsel zwischen Produktion und Standby erledigen. Zum Bedienen gibt es das Kommandozeilenwerkzeug *dgmgrl* oder den Enterprise Manager; der Autor hat mit der Kommandozeile bessere Erfahrungen gemacht. Interessant ist auf jeden Fall die Beobachtung der *alert.logs* beider Instanzen nach dem Absetzen eines Kommandos.

Data Guard Broker ist auch Voraussetzung für Fast Start Failover, eine mit 10.2.x eingeführte komplette Automatisierung des Failover-Prozesses. Aber Vorsicht: Vor der Einführung dieses Verfahrens sollte jeder Fall separat auf seine Tauglichkeit untersucht werden. Fast Start Failover setzt eine funktionierende Konfiguration des Data Guard Broker voraus. Zusätzlich zu den beteiligten Datenbanken ist ein Beobachter auf einem dritten Server notwendig, der in regelmäßigen Intervallen die Verfügbarkeit der Produktionsdatenbank überprüft. Ist sie nach einstellbaren Kriterien vom Beobachter nicht mehr kontaktierbar, aktiviert er automatisch die Standby-Datenbank.

Außer den erwähnten Funktionen Real Time Apply und Snapshot Standby brachte Oracle 11g weitere Neuerungen. Die FAL-Prozesse (Fetch Archive Log) sind in der Lage, auf der Standby-Datenbank fehlende Logs vor dem Netztransport zu komprimieren. Erstmals ist es möglich, Windows- und Linux-Datenbanken in einer Data-Guard-Konfiguration zu testen, vorher waren identische Betriebssysteme notwendig. Die Erstellung von Standby-Datenbanken verläuft durch die *from active database*-Klausel des *duplicate database*-Kommandos in RMAN wesentlich einfacher. Mit dieser Erweiterung ist ein Backup der Produktionsdatenbank zur Erstellung der Standby-Datenbank nicht mehr notwendig, denn der Server erzeugt es im Hintergrund und überträgt es per Netz. Für Datenbanken jenseits einer Größe von 10 GByte dürfte das jedoch nicht praktikabel sein.

Eine identische Kopie der Produktionsdatenbank in einem Notfallrechenzentrum zu betreiben, ist sicherlich für die meisten geschäftskritischen Anwendungen ein Muss. Wie passt aber Oracles „Real Application Cluster“ (RAC) in dieses Bild? Viele Benutzer vertreten die Meinung, dass RAC ähnliche Vorzüge wie Data Guard bietet: Da mehrere Instanzen die gleiche Datenbank verwenden, ist eine hohe Ausfallsicherheit gewährleistet. Laufen einige Instanzen in einem entfernten Rechenzentrum (Extended Distance Cluster), ist sogar im Katastrophenfall ein Teil des Cluster verfügbar.

Zum einen ist jedoch der Betrieb eines solchen Cluster mit hohen Kosten verbunden, da ein passendes clusterfähiges Dateisystem vorhanden sein muss (zum Beispiel Oracles Automatic Storage Management) und der Cluster Interconnect sehr kurze Latenzzeiten benötigt, weshalb in der Regel Dark Fibre zum Einsatz kommt. Zum anderen kann eine solche Konfiguration keine Benutzerfehler abfangen. Dies geht bisher nur durch das zeitverzögerte Anwenden der Redo Logs auf der physischen Standby-Datenbank. Data Guard ist daher nach Ansicht des Autors eine Ergänzung von RAC.

Fazit

Zur Absicherung unternehmenswichtiger Oracle-Datenbanken sollte eine physische Standby-Datenbank bereitstehen. Eine Produktionsdatenbank kann durchaus mehrere davon mit Redo-Informationen versorgen, damit sind komplexe Szenarien realisierbar. Die Wahl des Protection Levels hängt von den Anforderungen der Fachabteilungen ab, oftmals reicht schon die Standardeinstellung mit Real Time Apply auf der Kopie.

Maximum Protection ist ein zweischneidiges Schwert: Zwar schließt sie Datenverlust aus, alle Fehler, die den Redo-Transport zur Standby-Datenbank verhindern, lösen jedoch das Herunterfahren der Produktionsdatenbank aus. Außerdem bestätigt der Server Commits nicht, solange nicht alle notwendigen Informationen die Standby-Datenbank erreicht haben. Zwischenzeitliche Netzengpässe können deshalb den Durchsatz drücken.

Wie mit jeder Hardware, die nur im Fehlerfall – also hoffentlich nie – zum Einsatz kommt, ist es schwierig, dem Management die Notwendigkeit ihrer Beschaffung zu vermitteln. So gibt es leider viele Situationen, bei denen zu schwache Hardware für den Katastophenfall vorgesehen ist. Ein gut ausgelasteter aus acht Knoten bestehender RAC lässt sich eben nicht durch eine Standby-Konfiguration mit zwei Knoten ersetzen. (ck)

MARTIN BACH

ist Oracle-Datenbank-Administrator und arbeitet als Consultant mit Schwerpunkt Oracle Real Application Cluster, Hochverfügbarkeit und Disaster Recovery in Brighton/England.

Literatur

[1] Andrea Held; Datenbanken; Gute alte Zeiten; Oracle Flashback; *iX* 10/05, S. 150





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Stabile Software durch Architektur-Refactoring

Vorbeugen ist besser als heilen

Michael Stal

Auch Softwarearchitekturen unterliegen Erosionsprozessen, wenn sie kontinuierlich und unsystematisch wachsen. Schleichen sich dabei strukturelle Defizite ein, ist deren sofortige Bereinigung ratsam, weil sie sonst zu wuchern und sich zu verfestigen beginnen. Das probate Gegenmittel besteht aus regelmäßigem architektonischen Refactoring.

Beim Erstellen eines Kartenhauses fügt der „Baumeister“ eine Spielkarte nach der anderen an die bestehende Konstruktion. Wenn einzelne Karten dabei etwas in Schieflage geraten, hat das zunächst keine negativen Auswirkungen. Irgendwann ist das Bauwerk aber so instabil, dass eine weitere Karte genügt, um es zum Einsturz zu bringen. Die Moral von der Geschicht: Es ist besser, nicht auf Sand zu bauen, sondern auf stabilem Fundament.

Was hat all das mit Softwareentwicklung zu tun? Für die Erstellung von Softwareartefakten gilt obige Schlussfolgerung ebenfalls. Ständiges Erweitern von Softwaresystemen in einem Entwicklungsprozess führt unweigerlich zu architektonischer Erosion, also zu Systemen, die sich entweder als instabil erweisen oder unter ihrem eigenen Gewicht kollabieren. Auch unsystematische und späte Verbesserungen, oft neudeutsch als Patches oder Workarounds bezeichnet, reparieren lediglich Symptome statt das Problem an der Wurzel zu packen.

In einem inkrementellen Entwicklungsprozess (Abbildung 1) wächst das System Schritt für Schritt (englisch: piecemeal growth). Jeder Schritt selektiert eine Anforderung, beginnend mit den Prioritäten, bettet die resultierenden Softwareartefakte in den bestehenden Systemkontext ein, unterzieht das Ergebnis anschließend einer genauen Qualitätsprüfung und stabilisiert es vor der nächsten Iteration, bis am Ende der Iterationen die lauffähige Anwendung entsteht. Dieses Stabilisieren kennt der Softwareentwickler als Refactoring.

Refactoring in a Nutshell

Laut Martin Fowler handelt es sich beim Refactoring um die strukturelle Änderung von Programmcode, ohne dabei das Verhalten und damit die Semantik zu modifizieren. Zur Veranschaulichung soll ein einfaches Beispiel dienen: Alle Unterklassen der Basisklasse *Shape* definieren die Methode *void draw()*:

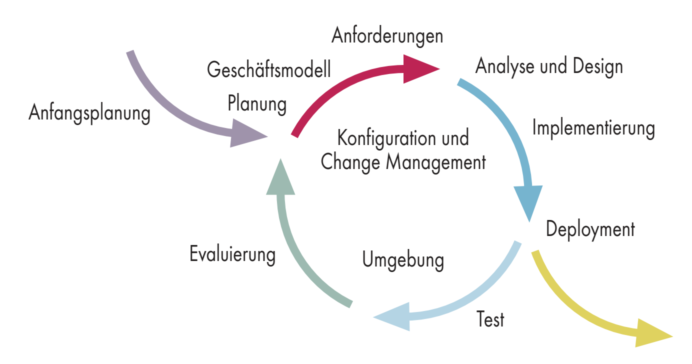
```
class Shape { }
class Circle: Shape {
  // ...
  public void draw() {
    // draw the Circle
  }
}
class Rectangle: Shape {
  public void draw() {
    // draw the Rectangle
  }
}
```

Offensichtlich gehört die Methode zu den inhärenten Eigenschaften aller *Shape*s. Es liegt daher nahe, die Operation in der Basisklasse zu verankern:

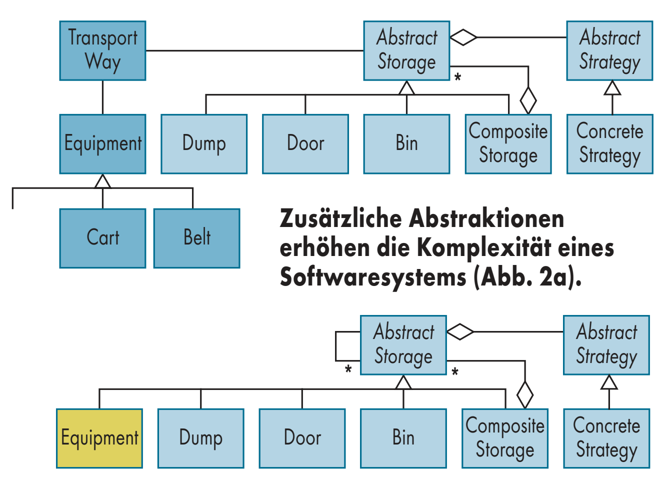
```
class Shape {
  public virtual void draw() { }
}
class Circle: Shape {
  // ...
  public override void draw() {
    // draw the Circle
  }
}
class Rectangle: Shape {
  public override void draw() {
    // draw the Rectangle
  }
}
```

Dieses einfache Code-Refactoring impliziert offensicht-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Architekturdesign sollte ein iterativer Entwicklungsprozess sein (Abb. 1).



Zusätzliche Abstraktionen erhöhen die Komplexität eines Softwaresystems (Abb. 2a).

Die Reduzierung überflüssiger Abstraktionen vereinfacht die Architektur des Systems (Abb. 2b).

lich eine Verbesserung im Programm-Code, ohne dessen äußeres Verhalten anzutasten.

Warum sollte sich aber Refactoring nur auf Programm-Code beschränken? Gerade das einführende Kartenhaus-Beispiel verdeutlicht, dass es sich um ein allgemeines Prinzip handelt. Allgemein definiert Refactoring jede Art von strukturverändernden, aber semantikinvarianten Transformationen.

Umbauen, wenn es riecht

Beim Architektur-Refactoring ist nicht die Implementierung Gegenstand der Verbesserungsmaßnahmen, sondern die Softwarearchitektur selbst. Ob die Notwendigkeit für architektonisches Refactoring besteht, erkennt der Architekt anhand sogenannter „smells“. Dieser Begriff stammt aus der Feder von Kent Beck, der eine Best Practice seiner Großmutter in Bezug auf Säuglinge zitiert: „If it smells, change it“. Von diesen unangenehmen „Gerüchen“ gibt es eine ganze Menge, weshalb hier nur ein kleiner Ausschnitt genannt werden soll.

Unzureichende Namen: Die Namen von Architekturartefakten sind so gewählt, dass darunter die Verständlichkeit der Architektur leidet.

Unnötige Abhängigkeiten: Im System tauchen unnötige Abhängigkeiten auf, die im Extremfall zu Abhängigkeitszyklen führen. Ein zirkuläre Abhängigkeit hemmt Faktoren wie Erweiter-, Änder- oder Testbarkeit, weil der Architekt jede Komponente im Zyklus nur zusammen mit den anderen am Zyklus beteiligten Komponenten betrachten kann.

Unnötige Abstraktionen: Starke Komplexität der Architektur entsteht oft durch unnötige Entitäten oder Beziehungen. Ein extremes Beispiel sind die sogenannten Entwurfsperlen.

Starke Kopplung oder schwache Kohäsion: Wenn zwischen zwei Subsystemen zahlreiche Beziehungen bestehen, stellt sich die Frage, wieso es sich überhaupt um separate Subsysteme handelt. Gleichermaßen weist schwache Kohäsion zwischen Komponenten in ein- und demselben Subsystem darauf hin, dass die Komponenten nur unzureichende semantische Zusammengehörigkeit besitzen.

Fehlende Symmetrie: Strukturelle Symmetrie in einer Architektur bedeutet, dass für die gleiche Aufgabe stets dieselben Lösungen zum Einsatz kommen. Auf der anderen Seite vermindert Asymmetrie die Verständlichkeit eines Softwaresystems, weil es nicht mehr genügt, nur wenige architektonische Ansätze zu verstehen.

Übergenerisches Design: Oft sind Softwarearchitekturen derart mit Variabilitäten überfrachtet, dass sie keine klare architektonische Vision mehr zeigen. Dazu gehören zum Beispiel Softwaresysteme, die am „Strategy-Syndrom“ leiden, also ungewöhnlich häufig das Strategy-Pattern nutzen.

Schwarze Löcher: Der Glaube an zentralistische Ansätze gipfelt bisweilen in zentralen Komponenten, die im Zentrum der Softwarearchitektur sitzen. Die „Hub-and-Spoke“-Architekturen aus der Enterprise Application Integration stellen ein typisches Beispiel dar. Derartige Ansätze führen nicht selten zu Skalierbarkeitsproblemen oder hoher Fehleranfälligkeit.

Do-it-Yourself: Der Erfindungsreichtum von Softwareentwicklern kennt bekanntlich keine Grenzen. Sobald aber statt bewährter Lösungen – etwa Patterns – fast überall Eigengewächse die Architektur überwuchern, besteht Handlungsbedarf.

Ein Exempel statuieren

Statt in der Theorie zu schwelgen, soll ein Fall aus der Praxis die Anwendung von Architektur-Refactoring illustrieren.

Das Problem: In der Architektur für ein Warenlagersystem hatten die Architekten eine Abstraktion namens „Abstract Storage“ eingeführt, von der sich die verschiedenen konkreten Warenspeicher, zum Beispiel Regale, ableiten (Abbildung 2a). Da der Wa-

iX-TRACT

- Kontinuierliches Erweitern von Softwarearchitekturen führt ohne regelmäßiges Refactoring zu architektonischer Erosion.
- Refactoring bezeichnet jede Form semantikerhaltender Restrukturierung. Während Code-Refactoring die Implementierung verbessert, optimiert Architektur-Refactoring die Softwarearchitektur.
- Architektonische „Smells“ wie fehlende Symmetrie sind Indikatoren für die Notwendigkeit von Architektur-Refactoring.
- Bei fortgeschrittenen architektonischen Problemen hilft Architektur-Refactoring nicht mehr, in dem Fall ist ein grundlegendes Reengineering erforderlich.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

rentransport ebenfalls zu den essenziellen Aufgaben eines solchen Logistiksystems gehört, kam später als weitere Abstraktion das Konzept des „Transport Way“ hinzu, was zu einer höheren Komplexität des Entwurfs führte.

Die Lösung: Nach ausgiebiger Reflexion erkannten die Architekten, dass Transportwege genau genommen eine andere Art von Warenspeicher darstellen. Sie vereinfachten daher die Architektur wie in Abbildung 2b, indem sie Transportausrüstung ebenfalls als Unterabstraktion von „Abstract Storage“ betrachteten.

Dieses Refactoring betrifft den architektonischen Smell „Unnötige Abstraktionen“ und erhält folgerichtig den Namen „Remove unnecessary Abstractions“. Darüber hinaus zeigt das Anwendungsbeispiel, dass Architekten zwischen den einzelnen architektonischen Verfeinerungen immer Refactoring-Schritte integrieren sollten. Je detaillierter sich die Architektur aus Abbildung 2a weiterentwickelt, desto höher die architektonische Erosion und damit der notwendige Restrukturierungsaufwand. Wie sagt der Arzt doch immer so einprägsam: „Vorbeugen ist besser als heilen.“

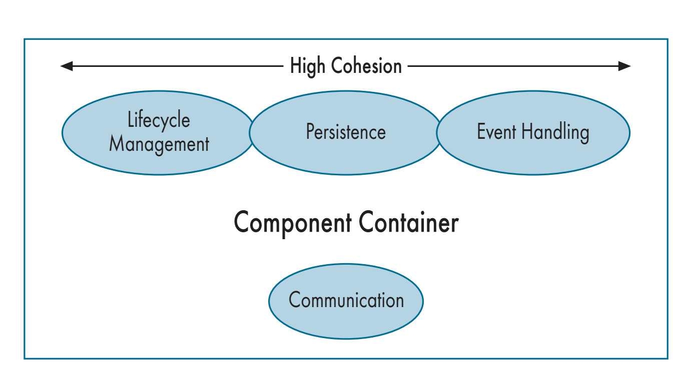
Mit dem Zweiten sieht man besser

Auch das zweite Refactoring-Beispiel entstammt einem realen Entwicklungsprojekt.

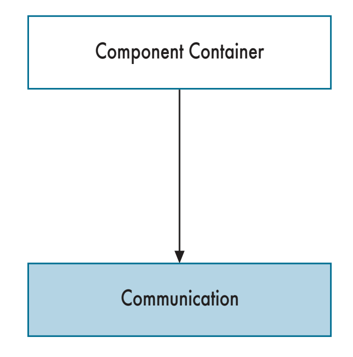
Das Problem: Bei der Entwicklung einer Container-Plattform für verteilte eingebettete Systeme war ursprünglich eine enge Integration zwischen Kommunikations-Middleware und Komponenten-Laufzeitumgebung angedacht (Abbildung 3a). Nach genauer Analyse erkannten die Entwickler, dass die Komponenten der Container-Umgebung wie „Lifecycle Management“ oder „Event Handling“ eng miteinander gekoppelt waren, während eine eher schwache Kohäsion zur Kommunikationsschicht bestand.

Die Lösung: Schwache Kohäsion zwischen Artefakten eines Subsystems bezeichnet einen architektonischen Geruch, der die Partitionierung in mehrere Subsysteme nahelegt. Im vorliegenden Fall haben die Architekten das Subsystem in zwei Systeme aufgeteilt, je eins für den Komponentencontainer und eins für die eigentliche Kommunikationsinfrastruktur (Abbildung 3b). Dadurch ließen sich später leichter Änderungen an den lose gekoppelten Subsystemen vornehmen.

Beide Anwendungsfälle zeigen, dass Refactorings Problem-Lösungs-Paare darstellen. Mit anderen Worten, es handelt sich um eine Art Restrukturierungs-Patterns. Wie Software-Patterns weisen Refactorings unterschiedliche Granularitätsebenen auf – beispielsweise Code- und Architektur-Refactorings – und können sogar vollständige Pattern-Systeme bilden.



Die Bindung zwischen dem Container und der Kommunikations-Middleware ist eher schwach (Abb. 3a).



Nach der Aufteilung in zwei Subsysteme lassen sich leichter Änderungen durchführen (Abb. 3b).

Besser zweiseitig als einseitig

Da Refactorings semantikinvariant arbeiten, lassen sie sich stets in zwei Richtungen betrachten. Hat zum Beispiel ein Entwicklungsteam eine eigene Lösung für Ereignismeldungen entwickelt, bei der die Ereignisquelle eine fest verdrahtete Liste der Ereignisempfänger enthält, liegt der architektonische Geruch „Do-it-Yourself“ vor. Eine bessere Lösung könnte sein, dass die Entwickler statt ihrer proprietären Lösung das Observer-Pattern anwenden, das dynamisches An- und Abmelden von Ereignis-Empfängern und auch eine weitgehende Entkopplung bietet. Für Geschäftsanwendungen erweist sich dieses Vorgehen als naheliegend und praktikabel. Hingegen dürfte sich der dynamische Lösungsansatz für eingebette Systeme oder Echtzeitsysteme nicht eignen. Dort würde man statt des Observer-Pattern lieber die fest verdrahtete Variante wählen, das Refactoring also eher in der umgekehrten Richtung anwenden. Beim Refactoring gibt es also kein Gut und kein Böse. Allein die architektonischen Anforderungen beeinflussen Notwendigkeit, Art und Richtung des Refactoring.

Wie bettet sich nun das beschriebene architektonische Refactoring in den Entwicklungsprozess ein? Vor und nach größeren Änderungen des Softwaresystems überprüfen die Architekten mit Code- und Design-Reviews das Ergebnis auf Qualitätsprobleme beziehungsweise architektonische „Smells“. Die Ermittlung und Visualisierung diverser Architektureigenschaften vereinfachen sich mit CQM-Werkzeugen (CQM = Code Quality Management) wie Sotograph spürbar. Liegen tatsächlich Erosionserscheinungen vor, wählen die Architekten die passenden Architektur-Refactorings. Sollten allerdings mehrere Maßnahmen notwendig sein, definiert sich deren Anwendungsreihenfolge nach folgenden Regeln, die auch schon den Architekturentwurf treiben:

Steuerung durch Prioritäten von Anforderungen: Alle Maßnahmen in Bezug auf Architekturartefakte, die sich auf Anforderungen mit höherer Priorität zurückführen lassen, haben Vorrang. Das ist im Übrigen ein weiterer triftiger Grund, warum Requirements Traceability beim Architekturdesign eine so wichtige Rolle spielt.

Strategische vor taktischen Refactorings: Aus dem gleichen Grund kommen Restrukturierungen strategischer Architekturentscheidungen vor allen taktischen Maßnahmen.

Architektur- vor Code-Refactorings: Natürlich ergibt es keinen Sinn, Code- vor Architektur-Refactorings zu platzieren. Schließlich könnten sich Teile der Implementierung nach einer Umstrukturierung der Architektur als obsolet erweisen.

Beim Architektur-Refactoring können zwei grundlegende Fälle auftreten. Existieren ausschließlich Designartefakte wie UML-Diagramme, betrifft das Refactoring lediglich den konzeptionellen Entwurf. Liegt der Architektur aber schon eine Implementierung zugrunde, führt jedes Architektur- not-

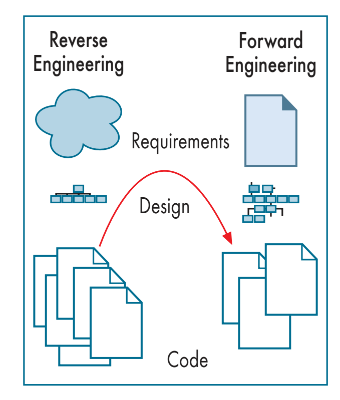
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

wendigerweise zu Code-Refactorings, weshalb die Umsetzung von Architektur- durch Code-Refactorings stets einer genauen Planung bedarf.

Selbstredend kann das Anwenden von Refactorings zu Fehlern führen, speziell wenn es manuell erfolgt. Im Sinne des TDD (Test-Driven Development) zählt daher eine Qualitätsprüfung nach jedem Refactoring zu den Pflichten der Softwareentwicklung. Gehört zur Architektur bereits eine Implementierung, lässt sich die Qualitätsprüfung durch einen Regressionstest realisieren. Bei einer Architektur ohne Implementierung gilt zwar Bertrand Meyers alte Regel „Bubbles don't crash", aber zumindest lassen sich Design-Reviews als Sicherheitsnetz nutzen. Die dritte Option bestünde darin, jeden Transformationsschritt durch mathematische Mittel zu verifizieren. Das aber dürfte nur für sicherheitskritische und gleichzeitig überschaubare Anwendungen infrage kommen.

Reengineering statt Refactoring

Wer eine Bruchbude erwirbt, dürfte nur selten auf die Idee kommen, das Haus mittels Refactoring-Maßnahmen in einen bewohnbaren Zustand zu versetzen – außer natürlich bekennende Anhänger des legendären Sisyphos. Der Experte macht sich zunächst ein Bild der Gesamtsituation, ermittelt, was auf der einen Seite zu retten ist und was auf der anderen einer Sanierung bedarf, berechnet, welche Kosten daraus entstehen würden, und erstellt eine detaillierte Planung. Auf betagte Softwaresysteme passt der beschriebene Ansatz ebenfalls.



Reengineering besteht aus Reverse Engineering und anschließendem Forward Engineering (Abb. 4).

Wenn also beispielsweise die Architektur eines wichtigen Softwaresystems weder dokumentiert noch bekannt ist, lokale Fehlerbeseitigung ständig zu neuen Fehlern führt, grundsätzliche Änderungen wie der Übergang von einer technischen Infrastruktur zu einer anderen sich nicht mehr einfach durchführen lassen, helfen Refactoring-Maßnahmen allein nicht mehr weiter. Stattdessen sollten Architekten und Entwickler einen Reengineering-Ansatz wählen, in dessen erster Phase Analyse und Reverse Engineering des alten Systems erfolgen und in dessen zweiter die als erhaltenswert befundenen Altteile in den Entwurf des neuen Systems einfließen (Abbildung 4).

Für die initiale Analyse kommt dabei die Methodik der SWOT-Analyse (Strengths, Weaknesses, Opportunities, Threats) zum Einsatz: Software-Ingenieure ermitteln und untersuchen alle existierenden Bestandteile des Softwaresystems hinsichtlich ihrer Stärken, Schwächen, Chancen und Risiken. Dadurch lassen sich erhaltenswerte Komponenten identifizieren, die sich im Idealfall unverändert nutzen lassen, im Normalfall aber einer „Renovierung" bedürfen, wofür Refactoring übrigens ein probates Hilfsmittel darstellt. Beim Reverse Engineering könnte sich natürlich herausstellen, dass keine Komponente des bisherigen Softwaresystems rettungswürdig erscheint, was eine komplette Neuentwicklung impliziert.

Hier zeigen sich die gravierenden Unterschiede zwischen Reengineering und Refactoring deutlich. Im Gegensatz zu Refactoring betrifft Reengineering das gesamte Softwaresystem, nicht nur lokale Bestandteile. Für Reengineering bedarf es eines Reverse-Engineering-Ansatzes, gefolgt von einem vollständigen Entwicklungsprozess für das neue System. Hingegen bettet sich Refactoring als fester Bestandteil in die einzelnen Iterationen ein. Als Ergebnis von Reengineering-Maßnahmen ergibt sich ein neues Softwaresystem, teilweise mit völlig verändertem Verhalten, während Refactoring zu lokalen Strukturänderungen führt, ohne das Verhalten anzutasten.

Fallstricke und Überzeugungstäter

Obwohl Refactoring einen so wertvollen Beitrag zur architektonischen Qualität leistet, gehört es noch nicht zu den Selbstverständlichkeiten der Softwareentwicklung. In diesem Zusammenhang sind aller „schlechten" Dinge drei.

Nicht jeder Projekt- oder Entwicklungsleiter neigt zu Überschwang, wenn er Zeit und Geld für Refactoring-Maßnahmen spendieren soll. Aber auch Entwickler und Architekten geben sich lieber der „Featuritis" hin statt sich mit ungeliebten Renovierungsmaßnahmen „aufzuhalten". Leider führt gerade diese Mentalität in den meisten Fällen zu Problemen. Und wie beim Testen gilt: Je später der Ansatz greift, desto größer die Folgekosten für notwendige Gegenmaßnahmen. Dass ständiges Erweitern von Softwaresystemen zur architektonischen Erosion führen muss, leuchtet erfahrenen Software-Ingenieuren unmittelbar ein.

Systematische Softwareentwicklung besteht darin, ein wenig zu entwerfen, ein wenig zu implementieren, das Erreichte zu überprüfen und gegebenenfalls zu refaktorisieren, um mit stabilem Unterbau in die nächste Iteration zu starten. Mit einem solchem Vorgehen des evolutionären Wachstums ist es unwahrscheinlich, dass sich von einer Iteration zur nächsten weitreichende Probleme in der Architektur ergeben, die sich nicht mit Refactoring angehen lassen. Refactoring erfolgt aber nur dann, wenn es explizit zur Verantwortung von Architekten und Entwicklern gehört und diese die dafür benötigte Zeit erhalten.

Ein berühmtes Zitat von Grady Booch lautet „A fool with a tool is still a fool". Allerdings gilt auf der anderen Seite ebenso, „An expert without a tool feels like a mule". Werkzeuge, die architektonisches Refactoring explizit und gezielt unterstützen, sind bislang Mangelware. Für das Erkennen architektonischer Gerüche empfehlen sich CQM-Werkzeuge, die auf Basis der Implementierung beispielsweise Metriken berechnen und Abhängigkeiten visualisieren.

Zu guter Letzt fehlt es heute schlicht an dokumentierten Architektur-Refactorings. Während der Softwareentwickler in Bezug auf Code-Refactoring auf ein breites Angebot von Maßnahmen zurückgreifen kann – teilweise sogar schon in Entwicklungsumgebungen integriert –, herrscht aufseiten des dokumentierten architektonischen Refactoring eher ein Mangelzustand. Lediglich Joshua Kerievsky bewegt sich mit seinem Buch „Refactoring to Patterns" [3] am äußersten Rande des Architektur-Refactoring.

Fazit

Um zum Eingangsbeispiel zurückzukehren: Wer ein Kartenhaus errichtet, sollte vor weiteren Baumaßnahmen immer wieder das aktuelle Zwischenergebnis stabilisieren. Geschieht dies nicht, können sich kleine Unregelmäßigkeiten soweit aufschaukeln, dass nur noch ein aufwendiges Reengineering Abhilfe schaffen und das Schlimmste verhindern kann. Das Mantra der agilen Softwareentwicklung verbietet schließlich unkon-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

trolliertes Wachstum und fordert stattdessen einen inkrementellen Ansatz kleiner Schritte, zu denen auch ausgiebige Refactoring- und Qualitätsmaßnahmen gehören.

Architektur-Refactoring ergänzt das inzwischen verbreitete Code-Refactoring um Restrukturierungsmaßnahmen für architektonisches Design, ist aber im Gegensatz zum weitverbreiteten Irrglauben, es sei etabliert, ein noch relativ neues und unerschlossenes Gebiet, zumindest was die Katalogisierung von Refactoring-Patterns betrifft. Trotzdem gibt es keine Ausrede für das fehlende Aufspüren von Teilen der Architektur, die Refactoring-Maßnahmen notwendig machen, beziehungsweise für das Unterlassen solcher Maßnahmen während des Architekturentwurfs. Inaktivität in diesem Kontext rächt sich garantiert – vielleicht nicht sofort aber mittel- bis langfristig. Der gute Vorsatz kann also nur lauten: Just do it! (ka)

DR. MICHAEL STAL

ist bei der Corporate Technology der Siemens AG als Principal Engineer tätig und beschäftigt sich mit verteilten Systemen und Softwarearchitekturen. Er ist unter anderem Koautor der Buchserie „Pattern-Oriented Software Architecture".

Onlinequellen

Martin Fowler; Refactoring Home Page
www.refactoring.com

Joshua Kerievsky; Refactoring to Patterns Home Page Interactive
industriallogic.com/rtpdata/index.html

Scott Ambler; Database Refactoring
databaserefactoring.com

Michael Stal; Software Architecture Blog
stal.blogspot.com

Definition von Refactoring auf der GI-Homepage
www.gi-ev.de/service/informatiklexikon/informatiklexikon-detailansicht/meldung/70/

Artikel von IBM zu Refactoring
www.ibm.com/developerworks/library/os-ecref/

Generelle Themen zu Softwarearchitekturen und Software Engineering beim Software Engineering Institute der Carnegie Mellon University
www.sei.cmu.edu/

Literatur

[1] Martin Fowler, Kent Beck, John Brant, William Opdyke, Don Roberts; Refactoring: Improving the Design of Existing Code; Addison-Wesley, 1999

[2] Serge Demeyer, Stéphane Ducasse, Oscar Nierstrasz; Object-Oriented Reengineering Patterns; Morgan Kaufmann, 2002

[3] Joshua Kerievsky; Refactoring to Patterns; Addison-Wesley, 2004

[4] Scott W. Ambler, Pramodkumar J. Sadalage; Refactoring Databases: Evolutionary Database Design; Addison-Wesley, 2006

iX-Link ix0810125



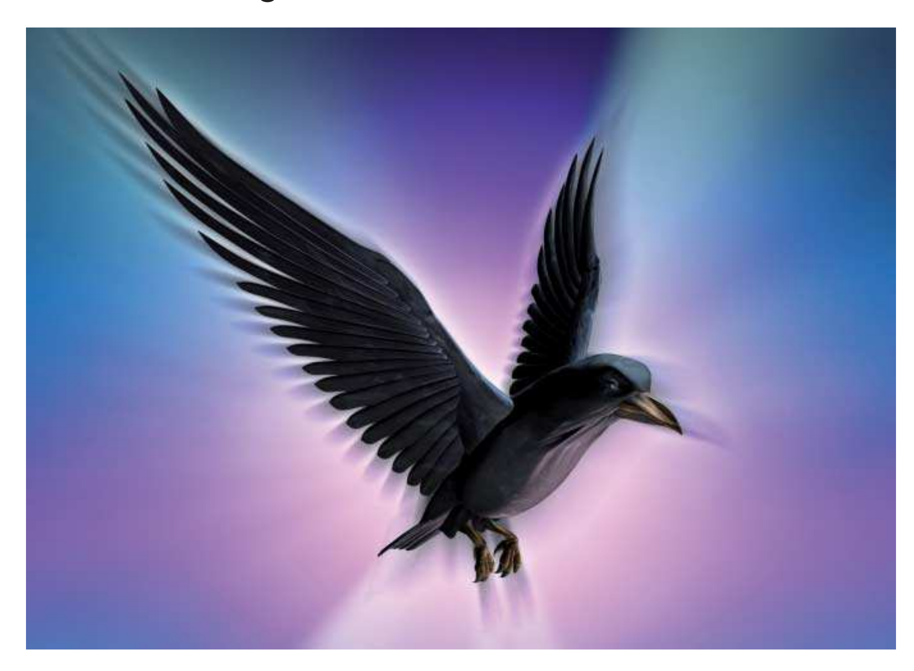


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Langzeit-Monitoring mit Munin

Der Rabe berichtet

Patricia Jung



Der Rabe Munin („Erinnerung“), in der nordischen Mythologie Bote des Gottes Odin, stand Pate bei der Entwicklung der Skriptsammlung Munin zum Langzeit-Monitoring numerischer Parameter. Ihr Einsatz empfiehlt sich nicht nur für Sysadmins, denn individuelle Überwachungs-Plug-ins sind schnell geschrieben.

Ob der Webserver Daten liefert oder der SSH-Zugang funktioniert, behalten Sysadmins gerne mit Nagios im Blick. Um Probleme frühzeitig zu erkennen, reicht es in vielen Fällen aber nicht aus, den Jetzt-Zustand zu erfassen. So liefert erst die Langzeitüberwachung des Netzwerkdurchsatzes frühzeitig Hinweise auf potenzielle Engpässe. In der Vergangenheit kam dazu vor allem Tobias Oetikers „Multirouting Traffic Grapher“ (MRTG, siehe „Onlinequellen [e]) zum Einsatz, der – wie der Name sagt – auf Netzwerkverkehr spezialisiert ist. Andere Wünsche wie die Überwachung der CPU-Last oder der Anzahl laufender Apache-Instanzen lassen sich damit nur durch Umschreiben des Quellcodes erfüllen. Daher konkurrieren mittlerweile mehrere Open-Source-(OSS-)Projekte um den Ruf, der flexibelste und würdigste Nachfolger zu sein, darunter eigenständige Applikationen wie Cricket [g] oder Cacti [h] sowie Nagios-Add-ons wie Nagiosgraph [i] und NagiosGrapher [j].

Ein Tool, das einerseits Leistungsdaten aufzeichnet und präsentiert, sich andererseits leicht in Nagios integrieren lässt (wie das geht, besprechen Gabriele Pohl und Michael Renner ausführlich in ihrem Buch [1]), ist Munin [a], ein OSS-Projekt, das im Jahre 2001 als LRRD (Linpro Round Robin Database) beim norwegischen OSS-Dienstleister Linpro (der derzeit mit der schwedischen Firma Redpill zu Redpill-Linpro verschmilzt) seinen Anfang nahm.

Round-Robin-Archive als Datenbasis

Munin nutzt das Perl-Modul aus dem RRDTool-Projekt [f] und erzeugt damit Datensammlungen in einem Binärformat, deren Größe sich nie ändert: Diese Round-Robin-Archive enthalten die Daten der vergangenen 48 Stunden in fünfminütiger Auflösung. Ältere Daten fasst Munin immer weiter zusammen, bis sie nach 16 Monaten ganz herausfallen. Daraus generiert Munin fortlaufend aktualisierte Tages-, Wochen-, Monats- und Jahresgraphen (Abb. 1). Deren Legende enthält für jeden Parameter den aktuellen (*Cur*), kleinsten (*Min*), größten (*Max*) sowie durchschnittlichen Wert (*Avg*) des Zeitraums.

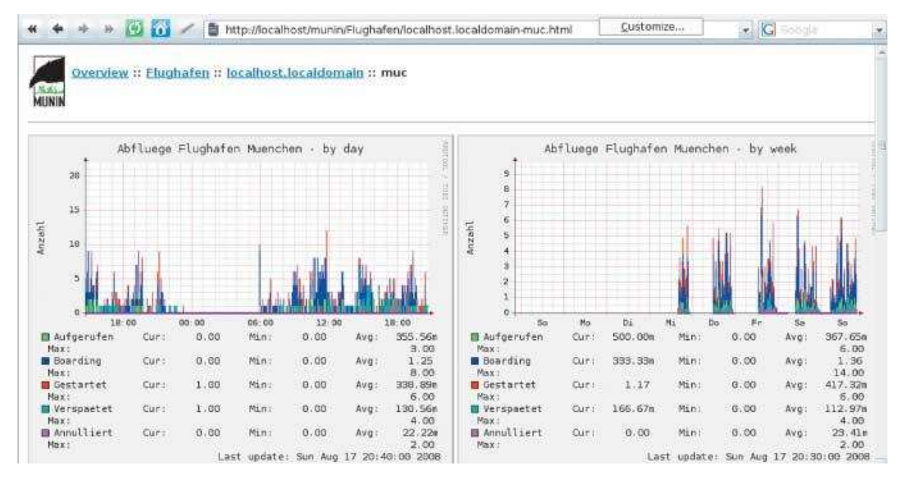
Wie andere RRD-basierte Tools eignet sich Munin daher nicht für Archivzwecke (wobei man sich natürlich zu Vergleichszwecken beispielsweise alle Monatsgraphen und die zugehörigen RRD-Archive zum Monatswechsel per Cronjob sichern kann). Es dient aber keineswegs nur zum Erfassen von Netzwerk- und anderen technischen Auslastungsdaten in IT-Infrastrukturen (und damit zum Capacity Planning nach ITIL), sondern ermöglicht das Langzeitmonitoring jeglicher numerischer Parameter, die sich per Skript abfragen lassen. Das können Verkaufszahlen oder der Google-Pagerank genauso sein wie – passende Messhardware vorausgesetzt – die Temperatur eines Raumes. Daher lassen sich auch Vertrieb, Marketing und andere nichttechnische Abteilungen schnell von der Nützlichkeit überzeugen.

Keine Rolle spielt das Aussehen des Monitoring-Skriptes, solange es seine Ausgaben in der von Munin erwarteten Form auf der Standardausgabe ausgibt.

iX-TRACT

- Grafische Auswertungen wiederkehrender (System-)Ereignisse helfen, frühzeitig Anomalien zu erkennen.
- Im Gegensatz zum weitgehend auf Netzwerkaspekte beschränkten MRTG lassen sich mit Munin fast beliebige numerisch repräsentierte Ereignisse überwachen.
- Aufgrund der eingesetzten Master-Node-Architektur kann die Überwachung vieler Rechner zentral auf einem System erfolgen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Die Tages- und Wochengraphen des in diesem Artikel entwickelten *muc*-Plug-in. Das *m* hinter den in der Legende genannten Werten steht für „Milli" (Abb. 1).

Listing 1: Lokale Abfrage per Telnet

```
$ telnet localhost 4949
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
# munin node at extrablatt.trish.de
list
open_inodes if_err_eth0 irqstats entropy processes
postfix_mailqueue if_eth0 df netstat interrupts swap
load cpu df_inode if_eth1 if_err_eth1 postfix_mailvolume
forks iostat open_files
memory vmstat
fetch netstat
active.value 582
passive.value 49
failed.value 0
resets.value 19
established.value 5
```

Listing 2: Plug-in-Beispielskript *muc*

```
#!/bin/sh
DEP_URL=http://www.munich-airport.de/de/consumer/fluginfo/
                              abflug/index.jsp?viewType=t
TMP_FILE=/tmp/.muc_flights
if test "$1" = "config"; then
   echo graph_title Abfluege Flughafen Muenchen
   echo graph_vlabel Anzahl
   echo graph_args --base 1000 --lower-limit 0
   echo graph_category Abflug
   echo calling.label Aufgerufen
   echo calling.draw AREA
   echo boarding.label Boarding
   echo boarding.draw STACK
   echo starting.label Gestartet
   echo starting.draw STACK
   echo late.label Verspaetet
   echo late.draw LINE2
   echo cancelled.label Annulliert
   echo cancelled.draw LINE2
else
   TIME=$(date +%H)
   MIN=$(echo "($(date +%M)/5)*5"|bc)
   case $MIN in
      0) TIME=$TIME:00 ;;
      5) TIME=$TIME:05 ;;
      *) TIME=$TIME:$MIN ;;
   esac
   TMP_FILE=$TMP_FILE:$TIME
   links -dump $DEP_URL | grep $TIME > $TMP_FILE
   echo "calling.value $(grep aufgerufen $TMP_FILE | wc -l)"
   echo "boarding.value $(grep boarding $TMP_FILE | wc -l)"
   echo "starting.value $(grep gestartet $TMP_FILE | wc -l)"
   echo "late.value $(grep geplant $TMP_FILE | wc -l)"
   echo "cancelled.value $(grep annulliert $TMP_FILE | wc -l)"
   rm $TMP_FILE
fi
```

Die Einbindung solcher Plug-ins ist eine Sache von (maximal) fünf Minuten.

Der Schlüssel zum Verständnis von Munin ist der, dass es *keine* Client-Server-Architektur implementiert (wie es selbst Kommentare im Makefile und auf Linpros eigener Feature-Seite [b] weismachen wollen), sondern nach dem Master-Node-Prinzip funktioniert: Auf dem Munin-Master lauscht nämlich kein Daemon. Stattdessen läuft dort alle fünf Minuten via Cron das Skript *munin-cron*, das nichts anderes tut, als vier Perl-Skripte aufzurufen.

Diese fragen die Daten von den zu überwachenden Rechnern ab und schreiben sie in RRD-Dateien (*munin-update*), warnen optional bei Grenzwertüber- oder -unterschreitungen (*munin-limits*), generieren Diagramme aus den in den RRD-Dateien abgelegten Graphen (*munin-graph*) und erzeugen respektive aktualisieren Webseiten mit der grafischen Präsentation (*munin-html*). Für deren Anzeige muss lokal ein Webserver laufen, es sei denn, die betreffenden Verzeichnisse sind für einen anderen Webserver remote zugänglich.

Sobald der Munin-Master über Port 4949 bei einem Node-Rechner anklopft, startet der dort laufende Daemon *munin-node* die gewünschten Plug-ins zunächst mit dem Argument *config*, um die abfragbaren Parameter zu ermitteln. Danach führt er sie im Messmodus aus und liefert die Standardausgaben zurück. Dabei ist es egal, ob diese Plug-ins Werte des Node selbst oder (etwa über SNMP) von Drittrechnern abfragen.

Die Aufgabe, die Graphen einzelnen Geräten zuzuordnen, übernimmt die Konfigurationsdatei des Masters, *munin.conf*. Sie legt somit nicht nur die zu überwachenden Rechner fest, sondern überschreibt bei Bedarf auch auf dem Node getroffene Einstellungen.

Insbesondere in den Fällen, in denen der Master nicht nur Node-Daemonen auf entfernten Rechnern, sondern auch auf dem eigenen abfragt, fällt es anfangs oft schwer, die ähnlich klingenden Konfigurationsdateinamen auseinander zu halten, denn jeder Node verfügt noch einmal über mindestens zwei: *munin-node.conf* regelt die Belange des *munin-node*-Daemon. Zusätzlich existiert ein Unterverzeichnis namens *plugin-conf.d*. Darin liegende Dateien liest *munin-node* in alphabetischer Reihenfolge aus, um die Laufzeitumgebung für seine Plug-ins zu konfigurieren. Per Default enthält *plugin-conf.d* eine Konfigurationsdatei mit dem unglücklich gewählten Namen *munin-node*.

Die Paketmanagementsysteme vieler Linux-Distributionen und BSD-Varianten erlauben es, Master und Node in getrennten Paketen zu installieren (detaillierte Installationshilfen, darunter für Mac OS X und Windows, geben Pohl und Renner [1]). So spielt man bei Debian/Ubuntu auf dem Master das Paket *munin*, auf allen Rechnern, auf denen Plug-ins Daten ermitteln sollen, *munin-node* ein. Dieses enthält auch die standardmäßig mitgelieferten Plug-ins, darunter eine Reihe selbstinstallierende.

Telnet auf Port 4949

Sind für deren Betrieb alle Voraussetzungen erfüllt, kann man die Daten lokal beim *munin-node*-Daemon abfragen, Listing 1 zeigt ein Beispiel. Bei Apache-Plug-ins, die bei der Installation keinen lokalen Webserver vorfinden, ist das beispielsweise nicht der Fall. Sie bleiben auch inaktiv, wenn man den *httpd* nachträglich startet. Über den Befehl *list* kann man sich die auf dem Node abrufbaren Plug-ins zeigen und via *fetch <plugin>* deren Daten ausgeben lassen.

Führt man den Kommandozeilenbefehl *munin-node-configure --suggest* auf dem Node-Rechner aus, liefert dieser Hinweise darauf, woran die Aktivierung eines installierten Plug-ins scheitert:

```
Plugin          | Used | Suggestions
[...]
apache_accesses | no   | [no apache server-status ↵
                   or Extended Status missing on ports 80]
```

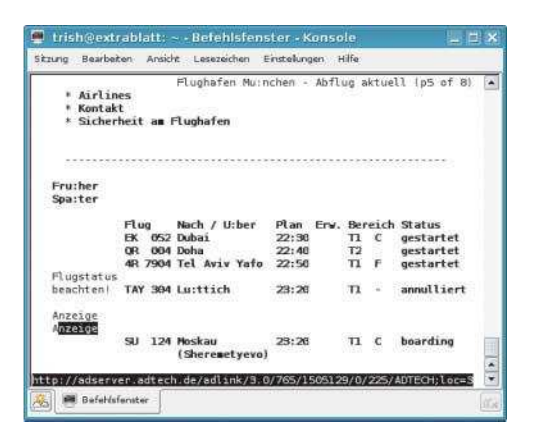
Allerdings klappt das nur, wenn das entsprechende Plug-in eine Methode namens *autoconf* mitbringt:

```
$ /[...]/munin/plugins/apache_accesses autoconf
no (no apache server-status or ExtendedStatus ↵
                              missing on ports 80)
```

Was Munin-Plug-ins können müssen

Wer vorhat, der Allgemeinheit eigene Plug-ins auf der Munin-Exchange-Plattform [c] zur Verfügung zu stellen, sollte *autoconf* implementieren, doch ein funktionsfähiges Monitoring setzt wesentlich

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Aus dieser (hier in *links* gezeigten) Webseite ermittelt *muc* die Anzahl der aktuell abgefertigten, gestrichenen und verspäteten Flüge (Abb. 2).

weniger voraus: Munin-Plug-ins müssen, ohne weitere Argumente aufgerufen, die gemessenen Parameter in der Form *<parametername>.value <wert>*, gefolgt von einem Newline-Zeichen auf der Standardausgabe ausgeben:

```
$ /[...]/munin/plugins/apache_accesses
accesses80.value U
```

Mit dem Wert U sagt *apache_accesses*, dass es den Wert des Parameters *accesses80* (derzeit) nicht ermitteln kann. Ruft man Plug-ins mit dem Argument *config* auf, verraten sie mindestens den Titel des Graphen (*graph_title*), die Beschriftung der Y-Achse (*graph_vlabel*), den Legendentext der überwachten Werte (*<parametername>.label*) und den RRD-Typ der Kurve (*<parametername>.type*, siehe [1] oder *man rrdcreate*), sofern dieser vom Default *GAUGE* abweicht:

```
$ /[...]/munin/plugins/apache_accesses config
graph_title Apache accesses
graph_args --base 1000
graph_vlabel accesses / ${graph_period}
graph_category apache
accesses80.label port 80
accesses80.type DERIVE
[...]
```

graph_args erlaubt es, mit Argumenten auf die Graphenerzeugungsroutine der RRDTools Einfluss zu nehmen (s. *man rrdgraph*). Sinnvoll ist es, mit *--base 1000* oder *--base 1024* anzugeben, auf welche Basis sich die der Maßeinheit vorangestellte Vorsilbe „Kilo“ bezieht. Graphen, deren Kategorie nicht in *graph_category* spezifiziert ist, ordnet die Munin-Webseite unter *Other* ein.

Einsatzbeispiel: Abflüge überwachen

Listing 2 zeigt ein Beispiel eines einfachen Shellskripts namens *muc*, das als Munin-Plug-in die Abflüge auf dem Münchner Flughafen überwacht. Es ermittelt mit *date +%H* sowie *date +%M* die aktuelle Stunde und Minute. Da nur volle fünf Minuten als Abflugzeiten Verwendung finden, rundet das Skript den Wert auf die letzten vollen fünf Minuten ab. Zwar läuft der Datensammel-Cronjob des Munin-Masters alle fünf Minuten, doch kann es passieren, dass die Abfrage des Plug-in auf belasteten Maschinen erst etwas später erfolgt.

Aus dem vom Textbrowser *links* gelieferten Textdump der aktuellen Abflugtabelle (siehe Abb. 2) sucht *grep* nach der so ermittelten Abflugzeit und schreibt die entsprechenden Zeilen in eine temporäre Datei. Aus dieser extrahiert wiederum *grep* die Zeilen, die jeweils zu aufgerufenen (*calling*), zum Einsteigen bereiten (*boarding*), gestarteten (*starting*), verspäteten (*late*) und gestrichenen (*cancelled*) Flügen gehören. Wie viele das zur letzten Abflugzeit jeweils waren, zählt in allen fünf Fällen *wc -l* zusammen:

```
$ ./muc
calling.value 0
boarding.value 1
starting.value 0
late.value 0
cancelled.value 1
```

In der Präsentation soll Munin die *calling-*, *boarding-* und *starting*-Werte übereinander stapeln: In Ermangelung der tatsächlichen Abflugzeiten wertet sie das Skript als im entsprechenden Fünfminutenintervall abgefertigte Abflüge. Passend dazu gibt *./muc config* für diese Parameter *<parametername>.draw STACK* aus.

Nur Flügen, die zum angegebenen Abflugzeitpunkt noch nicht aufgerufen waren, weist die Abflugtabelle einen neuen Termin zu und kennzeichnet sie vorerst als *geplant*. Da diese zu diesem neuen Termin noch einmal als abgefertigte Flüge in die Statistik eingehen, zeichnet das Skript sie separat als dicke Linie (*LINE2*) ein. Ebenso weist es die gestrichenen Flüge als eigene Linie aus.

Plug-ins aktivieren

Zum Aktivieren eines Plug-in verlinkt man es ins *plugins*-Verzeichnis des Node und startet dessen Daemon neu:

```
# ln -s </pfad/zu/>muc /etc/munin/plugins/muc
# /etc/init.d/munin-node restart
```

Damit lässt es sich auf dem Node per *telnet* mit dem Befehl *fetch* abfragen:

```
$ telnet localhost 4949
[...]
fetch muc
calling.value 0
boarding.value 1
starting.value 0
late.value 0
cancelled.value 1
```

Funktioniert dies, trägt man den neuen Node in die *munin.conf*-Konfigurationsdatei auf dem Master-Rechner ein, denn erst damit beginnt die Überwachung. Per Default enthält diese Datei einen Eintrag für *localhost* (127.0.0.1), sodass Munin die Daten eines auf dem Master-Rechner aktivierten Node sofort aufzeichnet:

```
[Flughafen;localhost.localdomain]
  address 127.0.0.1
  use_node_name yes
```

Welcher Node das ist, legt der Parameter *address* fest, der zu jedem mit einer eckigen Klammer beginnenden Überwachungsauftrag gehört. Wie in Abbildung 3 zu sehen ordnet die Munin-Webseite die Überwachungsgraphen in einer einstufigen Hierarchie an: Jeder überwachte Rechner trägt einen Namen (hier *localhost.localdomain*) und gehört zu einer Gruppe (hier *Flughafen*). Beide Parameter entnimmt der Munin-Master den eckigen Klammern: Steht vor einem als Name angegebenen Fully Qualified Domain Name (FQDN) kein durch Semikolon (aber ohne Leerzeichen) abgetrennter Gruppenname, dient der rechts des ersten Punkts stehende String (der Domain-Anteil) als solcher.

Ob der dazu gehörende Rechner im Netz tatsächlich mit dem in eckigen Klammern angegebenen Host-Namen oder FQDN zu erreichen ist, spielt keine Rolle. Das gibt Flexibilität: So kann

Listing 3: Reparatur per *rrdtool*

```
$ rrdtool dump /var/lib/munin/Flughafen/localhost.localdomain-muc-boarding-g.rrd
[...]
   <!-- 2008-08-13 21:00:00 CEST / 1218654000 --> <row><v> 0.0000000000e+00 </v></row>
   <!-- 2008-08-13 21:05:00 CEST / 1218654300 --> <row><v> 4.8797675500e+00 </v></row>
   <!-- 2008-08-13 21:10:00 CEST / 1218654600 --> <row><v> 1.0973450533e+00 </v></row>
[...]
```

Listing 4: Erweiterung für *muc*

```
UNIXTIME=$(date -d$TIME:00 +%s)
echo "calling.value $UNIXTIME:$(grep aufgerufen $TMP_FILE | wc -l)"
echo "boarding.value $UNIXTIME:$(grep boarding $TMP_FILE | wc -l)"
echo "starting.value $UNIXTIME:$(grep gestartet $TMP_FILE | wc -l)"
echo "late.value $UNIXTIME:$(grep geplant $TMP_FILE | wc -l)"
echo "cancelled.value $UNIXTIME:$(grep annulliert $TMP_FILE | wc -l)"
```


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

man die Daten eines Rechners, den ein nicht lokal laufender Node (beispielsweise per SNMP) überwacht, unter seinem richtigen Namen einordnen statt unter dem des Node-Rechners. (Zu diesem Zweck setzt man außerdem den Parameter *use_node_name* auf *no*.)

Dass man sich dennoch von vornherein über den Gruppennamen klar sein sollte, hat einen anderen Grund: Der Munin-Master verwendet diesen als Namen des Verzeichnisses, in dem er die zugehörigen RRD-Dateien und Graphen ablegt. Erstere landen unter Debian in */var/lib/munin/Flughafen/*, Letztere in */var/www/munin/Flughafen/*; das Basisverzeichnis kann je nach Installation variieren.

Der in den eckigen Klammern angegebene Name findet sich im Dateinamen der RRD-Dateien und Graphen wieder: So heißt die RRD-Datei, die die Werte des vom Plug-in *muc* ermittelten Parameters *calling* auf *localhost.localdomain* aufnimmt, *localhost.localdomain-muc-calling-g.rrd*. Das *g* steht für den Default-Datentyp *GAUGE*. Wer Gruppe und Host-Bezeichnung nachträglich ändert und die bislang gesammelten Daten behalten will, muss diese RRD-Dateien zunächst umkopieren.



Munins Darstellungshierarchie orientiert sich an den Gruppennamen. Unter dem Label *Abflug* befinden sich die Daten des Skripts *muc* (Abb. 3).

Reparaturarbeiten an RRD-Dateien

Abgesehen davon, dass man im laufenden Betrieb stets nur maximal fünf Minuten Zeit hat, um Fehler in einer Round-Robin-Datenbank zu korrigieren, lässt sich dies relativ unproblematisch und gegebenenfalls skriptgesteuert erledigen. Listing 3 zeigt den dazu benötigten Aufruf, der die zum Parameter *boarding* gehörende RRD in XML-Form auf der Standardausgabe ausgibt. Hier ist deutlich sichtbar, dass die Datenbank statt der vom Skript gelieferten Ganzzahlen (hier 5 und 1) leicht abweichende Gleitkommawerte enthält. Das hängt damit zusammen, dass RRDTool Werte, die nicht exakt zur geplanten Zeit eintreffen, auf die Planzeit interpoliert speichert.

Im vorliegenden Anwendungsfall erweist sich dieses Verhalten als Bug, dem sich mit einem zwischengeschalteten Datenbankkorrekturskript abhelfen ließe.

```
$ rrdtool restore <datei>.xml <datei>.rrd
```

wandelt eine korrigierte XML-Datei ins Binärformat zurück. Da *rrdtool restore* keine existierenden RRD-Dateien überschreibt, muss man den Umweg über eine temporäre Datei wählen, mit der man das Muninsche RRD-Archiv später überschreibt. Dabei gilt es zu beachten, dass sich Besitzer und Gruppe – meist *munin:munin* – nicht verändern.

Für eine gründliche Behebung dieses Problems benötigt man Munin in einer Version ab 1.3.4. RRDTool erlaubt es nämlich explizit, dem übermittelten Wert mit Semikolon getrennt den Zeitpunkt in Sekunden seit dem 1.1.1970 00:00:00 UTC voranzustellen, für den er gilt. Dazu verändert man den Code des *muc*-Plug-in zwischen dem *links*- und dem *rm*-Aufruf etwa wie in Listing 4 gezeigt. Munin kommt damit erst ab Version 1.3.4 zurecht. Die nicht abwärtskompatible Ausgabe des Plug-in sah am 15. August zwischen 13:25:00 und 13:29:59 streikbedingt so aus:

```
$ ./muc
calling.value 1218799500:0
boarding.value 1218799500:0
starting.value 1218799500:0
late.value 1218799500:1
cancelled.value 1218799500:0
```

Ausbaumöglichkeiten

Nach weiteren Ausbaumöglichkeiten für das Skript muss man nicht lange suchen: Um es zum Monitoring verschiedener Flughäfen einzusetzen, würde man es zu einem Wildcard-Plug-in ausbauen, bei dem der Name des Links in */etc/munin/plugins* festlegt, was Munin konkret misst. Statt die abzufragenden URLs fest im Skript zu verankern, ließe es sich so umschreiben, dass es diese aus den in den Dateien unter */etc/munin/plugin-conf.d/* definierten Umgebungsvariablen ausliest. Da beides die Komplexität des Skripts deutlich erhöht, wären dann auch die Zeiten vorbei, in denen sich fehlende Dokumentation rechtfertigen lässt.

Bei all diesen und weiteren Vorhaben bieten neben dem genannten Buch [1] das englischsprachige Munin-Wiki [a] sowie die englisch- [d] und deutschsprachigen Mailinglisten [d] Hilfe an. (avr)

Onlinequellen

[a]	Munin-Wiki	munin.projects.linpro.no
[b]	Linpros Produktseite	www.linpro.no/en/produkter_og_loesninger/aapen_kildekode_prosjekter/munin
[c]	Munin-Exchange	muninexchange.projects.linpro.no
[d]	Mailingliste EN [DE]	https://lists.sourceforge.net/lists/listinfo/munin-users[-de?language=de]
[e]	MRTG	oss.oetiker.ch/mrtg
[f]	RRDTool	oss.oetiker.ch/rrdtool
[g]	Cricket	cricket.sourceforge.net
[h]	Cacti	www.cacti.net
[i]	Nagiosgraph	nagiosgraph.sf.net
[j]	NagiosGrapher	sourceforge.net/projects/nagiosgrapher/

Literatur

[1] Gabriele Pohl, Michael Renner; Munin – Graphisches Netzwerk- und System-Monitoring; ISBN 978-3-937514-48-2, Open Source Press 2008





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Tutorial: Active Directory auch für Unix und Linux

Diener zweier Herren

Mark Pröhl, Michael Weiser

Je größer die Computerlandschaft, desto komplexer gerät die Administration. Vor allem in gemischten Umgebungen laufen selbst einfache Aufgaben wie die Verwaltung von Benutzerdaten schnell aus dem Ruder. Mit etwas Aufwand lässt sich ein vorhandenes Active Directory auch auf Unix- und Linux-Systemen für diese Zwecke verwenden.

In fast jedem Windows-Netz ernst zu nehmender Größe erledigt heute Active Directory (AD) die Benutzerverwaltung, während zum Beispiel in gewachsenen Unix-Umgebungen nach wie vor der Network Information Service (NIS) verbreitet ist. Zwar existieren seit Langem Techniken, beide Welten synchron zu halten – AD etwa kann aus seinen Nutzerdaten über die Services for Unix (SFU) NIS-Maps generieren –, in der Praxis jedoch trifft man nur allzu oft auf getrennt verwaltete Windows- und Unix-Umgebungen.

Für dieses Tutorial soll die Firma für „Neue, innovative Service- und Applikationsdienstleistungen“ (NiS-AD) als fiktives, aber durchaus typisches Beispiel dienen. Das Unternehmen betreibt intern ein Netz aus Windows-PCs, Linux-Desktops und verschiedenen Servern mit kommerziellen Unix-Varianten. Für die Windows-Rechner existiert bereits ein zentrales Active Directory. Getrennt verwaltete NIS-Maps versorgen die übrigen Rechner mit den Benutzerinformationen. Stand lange Zeit der Wunsch nach einheitlichem Identitätsmanagement dem ehernen IT-Grundsatz „never touch a running system“ gegenüber, rümpfen immer öfter die Auditoren ihre Nase über das veraltete NIS und seine prinzipiellen Schwachstellen. Letztere sind inzwischen nicht mehr nur potenzielle Risiken, sie kosten mitunter bares Geld. Seit Anfang 2007 gelten für die Banken aller EU-Staaten die sogenannten Basel-II-Richtlinien: Als Folge davon ist nun die Sicherheit der IT-Infrastruktur eines der Kriterien, mit dem Banken die Bonität von Unternehmen beurteilen. Sichere Netze erlauben günstigere Kredite.

Für NiS-AD ist daher nun die Zeit gekommen, das bewährte NIS für die Unix-Welt abzulösen und statt dessen das bestehende Active Directory auf sämtliche Rechner auszudehnen. Dadurch, so hofft die Firma, lässt sich die Verwaltung der Benutzerinformationen vereinheitlichen, die Sicherheitsanforderungen der Auditoren sind erfüllt und ganz nebenbei winkt auch dem Unix- oder Linux-Benutzer in einer AD-Umgebung mehr Komfort durch sogenanntes Single Sign-On. Wie das im Detail aussieht, untersucht die IT-Abteilung in einem dreistufigen Migrationsprojekt (siehe Kasten „Tutorialinhalt“): Teil eins beschäftigt sich allein mit den Benutzerpasswörtern, die künftig nicht mehr im NIS gepflegt werden. Statt dessen soll die Überprüfung der Passwörter mithilfe der zentralen AD-Server erfolgen. In der zweiten Stufe sollen auch alle übrigen Benutzerinformationen aus dem NIS ins AD wandern. Zum Abschluss des Projektes binden die Administratoren schließlich bestehende Unix-Dienste direkt an AD an, um den Benutzern überflüssige Passworteingaben zu ersparen.

Oldie NIS mit strukturellen Schwächen

Im ersten Teilprojekt werfen die Administratoren zunächst einen Blick auf den Ist-Stand: Meldet sich ein Benutzer an einem Unix-Rechner an, generiert der aus dem eingegebenen Passwort eine verschlüsselte Zeichenkette und vergleicht sie mit einem vorab hinterlegten Wert. Der kann in einer lokalen Datei stehen wie */etc/passwd* oder */etc/shadow*. In größeren Umgebungen ist es jedoch einfacher, das verschlüsselte Passwort über einen Netzdienst zu verteilen, statt viele einzelne Dateien zu pflegen. Im NiS-AD-Netz gibt es dazu die NIS-Map *passwd*. Das Vorgehen hat jedoch ein prinzipielles Problem: Jeder Rechner entscheidet für sich, ob das eingegebene

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Passwort korrekt war oder nicht. Dazu benötigt er Zugriff auf die verschlüsselten Passwörter sämtlicher Benutzer. Wer in den Besitz der Passwortliste gelangt, kann durch eine Brute-Force- oder Wörterbuch-Attacke versuchen, einzelne Passwörter zu knacken. Ein potenzieller Angreifer benötigt dazu entweder lokale Administratorrechte auf einem beliebigen Unix-Rechner, oder er muss den – unverschlüsselten – Netzverkehr zum NIS-Server abfangen können. Im Netz von NiS-AD geht es sogar noch einfacher: Da die verschlüsselten Passwörter in der allgemein lesbaren NIS-Map *passwd* gespeichert sind, genügt hier ein einfaches *ypcat passwd* als „Hackertool“, das jedem gewöhnlichen Benutzer zur Verfügung steht.

Umgekehrt kann ein Angreifer auch versuchen, einem NIS-Client-Rechner einen anderen NIS-Server mit gefälschten Passwortdaten unterzuschieben. NIS sieht keine besonderen Sicherheitsmechanismen vor, mit der ein Client die erhaltenen Daten auf Echtheit prüft. Je nach Konfiguration bürgt einzig die IP-Adresse des Servers für authentische Informationen. Viele Clients machen es potenziellen Angreifern sogar noch einfacher und vertrauen schlicht jedem Rechner, der von sich behauptet, ein zuständiger NIS-Server zu sein.

Verbesserte Sicherheit durch Kerberos

Dass sich all diese Probleme sehr wohl vermeiden lassen, zeigt der als Teil von AD verwendete Mechanismus zur Passwortüberprüfung: das Authentifizierungsverfahren Kerberos [1]. Die komplette Liste der Benutzerpasswörter kennen dort nur noch speziell abgesicherte und dadurch besonders vertrauenswürdige Server. Im Kerberos-Jargon heißen sie KDC (Key Distribution Center), AD spricht allgemein von Domänencontrollern (DC). Will sich ein Benutzer einloggen, meldet der lokale Rechner das an einen Domänencontroller weiter und erhält von dort ein sogenanntes Ticket, sowie weitere, mit dem Passwort des Benutzers verschlüsselte Informationen zurück. Lassen die sich mit dem lokal eingetippten Passwort entschlüsseln, hat der Benutzer seine Identität erfolgreich nachgewiesen und darf üblicherweise ins System. Bei diesem Verfahren kommt ein Client-Rechner nicht mehr in den Besitz der kompletten Passwortliste aller Benutzer. Hat ein Angreifer Zugriff auf einen Client, kann er daher zwar nach wie vor Passwörter ausspähen, indem er beispielsweise alle Tastatureingaben abfängt. Doch das betrifft nur noch die Benutzer, die an dem gehackten Rechner arbeiten. Die Passwörter aller anderen Benutzer in der Domäne bleiben geschützt.

Um in den Genuss dieser Vorzüge zu kommen, müssen die Administratoren bei NiS-AD zunächst dafür sorgen, dass alle bisherigen Unix-Benutzer auch ein AD-Konto erhalten. Das ist weniger ein technisches, als vielmehr ein logistisches Problem, denn die AD-Kerberos-Implementierung verwendet andere Hash- und Verschlüsselungstypen als die bestehende *passwd*-NIS-Map. Das bisherige Unix-Passwort eines Benutzers lässt sich deshalb nicht einfach übernehmen. Für die Administratoren bedeutet das konkret, dass sie einen Weg finden müssen, zum Umstellungszeitpunkt sämtlichen Unix-Benutzern ein neues, initiales Passwort zukommen zu lassen. Weniger Probleme bereitet in der Regel das Übertragen der Benutzerdatenbank von NIS nach AD. Microsoft stellt dazu auf Domänencontrollern als Teil des „Identity Management for Unix“ (*idmumgmt.msc*) den grafischen „NIS Data Migration Wizard“ zur Verfügung, der unter anderem für jeden Nutzereintrag der *passwd*-NIS-Map einen neuen AD-Benutzer anlegen kann. Von der Kommandozeile aus erledigt *nis2ad* dieselben Aufgaben. Wer lieber von Unix aus arbeitet, kann mit Werkzeugen wie *adtool* (siehe „Onlinequellen“, [a]) recht einfach eigene Skripte erstellen, die die bestehenden Unix-Nutzerdaten im AD abbilden. Fürs Erste genügt es, einfach nur ein Benutzerkonto anzulegen und ein initiales Passwort zu setzen. Schwierig wird es, wenn verschiedene Benutzer auf Windows- und Unix-Seite bislang denselben Nutzernamen verwenden – einer von beiden muss weichen und sich mit einem neuen Namen seines Kontos anfreunden.

iX-TRACT

- Ohne zentrale Benutzerverwaltung läuft in heterogenen Umgebungen die Systemverwaltung schnell aus dem Ruder.
- Mit den Anforderungen nach Basel II wirken sich die strukturellen Sicherheitslücken von NIS auch wirtschaftlich aus.
- Eine vorhandene Active-Directory-Umgebung lässt sich auch für die Authentifizierung auf Linux-/Unix-Systemen verwenden.

Tutorialinhalt

Tickets beweisen die Identität

Weil im NiS-AD-Beispielnetz keine Dubletten zwischen Unix- und Windows-Nutzernamen vorkommen, können sich die Administratoren dort nach dem Anlegen der Unix-Benutzer im AD gleich darum kümmern, den Kerberos-Ticketaustausch zwischen Unix-Rechnern und Domänencontrollern in Gang zu bringen. Die gängigen kommerziellen Unix-Varianten bringen die nötigen Werkzeuge bereits in der Grundinstallation mit. Unter Linux und anderen freien Varianten muss der Administrator je nach Distribution noch Pakete wie *krb5-client* oder *krb5-user* nachinstallieren. Wichtig ist dabei vor allem */etc/krb5.conf*, die zentrale Konfigurationsdatei der Kerberos-Client-Bibliothek, Listing 1 zeigt ein Beispiel. Dort erfährt der Unix-Rechner, welcher sogenannten Kerberos-Realm er angehört – im Fall von AD ist das schlicht der Name der Domäne. Und er bekommt mitgeteilt, unter welcher Adresse er die zugehörigen Domänencontroller erreicht.

Eine Minimalversion wie in Listing 1 genügt bereits, um einem Unix-Rechner der NiS-AD-Beispielumgebung Kerberos-Anfragen an die AD-Domänencontroller zu ermöglichen. Der *realms*-Abschnitt kann entfallen, wenn der Unix-Rechner die DC auch als Nameserver verwendet. Die nötigen Informationen besorgt sich die Kerberos-Bibliothek dann über spezielle DNS-Anfragen.

Ob alles geklappt hat, testen die NiS-AD-Administratoren mit dem Testkonto „unixuser“, das sie zuvor im AD angelegt haben. Das auf dem Unix-Rechner ausgeführte Kommando *kinit unixuser* fordert beim AD-Controller ein initiales Kerberos-Ticket an, ausgestellt für den Benutzer „unixuser“. Es erscheint eine Abfrage, in der man das Windows-Passwort von „unixuser“ eingibt. Wie in Listing 2 zu sehen, zeigt der Aufruf *klist -5* danach ein gültiges Ticket für „unixuser“ an. Geht an dieser Stelle etwas schief, liegt das meist dar-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Domänenbeitritt von Unix-Rechnern

Der im Haupttext beschriebene Weg, einen Unix-Rechner in die Domäne eines Active Directory aufzunehmen, ist die ausführliche Variante, die alle nötigen Schritte von Hand ausführt: Maschinenkonto im Active Directory anlegen, *ServicePrincipalName* setzen, Maschinenkonto zurücksetzen, Maschinenpasswort ändern sowie die Keytab passend zum neuen Maschinenpasswort erstellen und auf dem Unix-Rechner hinterlegen. Das Vorgehen bietet große Flexibilität und lässt sich beispielsweise ganz analog auch für Dienstkonten anwenden. Mit dem Hilfsprogramm *krb5servicetool* [d] kann sich der Administrator ein wenig Arbeit ersparen und die letzten beiden Schritte automatisieren. Allerdings bleibt der Nachteil, das Passwort des Maschinenkontos vorübergehend auf einen trivialen Wert zu setzen. Während dieses Zeitfensters könnte ein Angreifer sich erweiterte Rechte zum Active Directory beschaffen.

Das Risiko lässt sich vermeiden, wenn der Administrator auf einem Windows-Rechner das Kommando *ktpass.exe* verwendet, um die Keytab für den Unix-Rechner zu erzeugen. Microsoft stellt *ktpass* als Teil der Windows Support Tools [b] frei zur Verfügung. Die so generierte Keytab muss der Administrator jedoch noch manuell auf einem möglichst sicheren Weg zum Zielrechner übertragen.

Mit Samba kann man seit Version 3 den Beitritt zu einer Active-Directory-Domäne direkt vom Unix-Rechner aus initiieren. Dem Samba-Aufruf *net ads join* genügen dazu wie beim Windows-Pendant Name und Passwort eines administrativen Benutzerkontos. Damit Samba das Computerpasswort nicht nur in seiner eigenen TDB speichert, sondern zur friedlichen Koexistenz mit anderen kerberisierten Diensten auch eine *Keytab*-Datei anlegt, muss die *smb.conf* den Eintrag *use kerberos keytab = yes* enthalten. Das Format der damit erhaltenen Keytab-Datei ist jedoch stark von der eingesetzten Samba-Version abhängig. Die Option *use kerberos keytab* bietet Samba seit Version 3.0.6.

Wer sonst kein Samba benötigt und allein für den Domänenbeitritt keine komplette CIFS-Suite installieren möchte, kann auf *msktutil* [c] zurückgreifen. Dem freien Hilfsprogramm für Unix und Linux genügt ein gültiges Kerberos-Ticket eines administrativen Benutzers, um Client-Rechner vollautomatisch in eine Active-Directory-Domäne zu integrieren. Weitere Optionen ändern das aktuelle Computerpasswort oder verwalten die *ServicePrincipalNames*.

an, dass der Client-Rechner die konfigurierten Host-Namen der Domänencontroller nicht auflösen kann oder dass die Systemzeit auf Domänencontroller und Client sich unterscheidet. Nicht umsonst empfehlen Praktiker für Kerberos-basierten Umgebungen den Einsatz von NTP (Network Time Protocol) für die Synchronisierung der Systemuhren.

PAM-Konfiguration für Kerberos aufbohren

Nachdem Kerberos auf den Unix-Rechnern grundsätzlich funktioniert, gilt es als Nächstes, die Systemanmeldung umzustellen. Statt wie bisher die Passwörter beim Login in einer NIS-Map nachzuschlagen, sollen die Maschinen Kerberos-Tickets vom AD-Domänencontroller anfordern und überprüfen. Nahezu alle freien und kommerziellen Unix-Derivate erlauben es inzwischen, die Benutzeranmeldung über Pluggable Authentication Modules (PAM) flexibel zu konfigurieren. AIX verwendet standardmäßig ein separates, vom prinzipiellen Aufbau aber mit PAM vergleichbares System, die Loadable Authentication Modules (LAM). Egal ob LAM oder PAM, für beide Varianten überprüft das Standardmodul in der Grundkonfiguration das eingetippte Benutzerpasswort anhand einer Tabelle, die es etwa aus */etc/passwd*, */etc/shadow* oder einer NIS-Map bezieht.

Um die Anmeldung an AD anzubinden, installiert und konfiguriert der Administrator ein Zusatzmodul, das das Kerberos-Verfahren beherrscht. Das nötige Modul heißt bei PAM beispielsweise *pam_krb5* und ist für alle gängigen Betriebssysteme verfügbar. Allerdings können sich Syntax und Funktionsumfang der einzelnen *pam_krb5*-Implementierungen je nach Betriebssystem und Distribution etwas unterscheiden. Listing 3 zeigt am Beispiel eines Linux-Rechners, welche Änderungen typischerweise an der PAM-Konfiguration nötig sind. Änderungen im Vergleich zum typischen Auslieferungszustand sind fett hervorgehoben. Die Option *minimum_uid* stellt sicher, dass sich Systembenutzer wie *root* nach wie vor über ein lokales Verfahren anmelden. Das verhindert Hakeleien, falls die Netzverbindung zum Kerberos-Server gestört sein sollte. *use_first_pass* verhindert doppelte Passwortabfragen. Die PAM-Konfiguration befindet sich in */etc/pam.d/* und ist je nach Distribution auf verschiedene Dateien verteilt.

Auf das bisherige Standardmodul *pam_unix* kann man auch nach der Umstellung nicht verzichten, da Systembenutzer wie *root* sich mitunter auch dann anmelden müssen, wenn keine Netzverbindung zum Domänencontroller besteht und die das System deshalb nach wie vor lokal in */etc/passwd* verwaltet. Wer sicherstellen möchte, dass alle im AD verwalteten Benutzer sich lediglich kerberisiert anmelden können, sollte deshalb deren altes Passwort in der NIS-Map *passwd* entfernen und durch „*“ oder einen anderen ungültigen Eintrag ersetzen.

Absicherung gegen Netzangriffe

Damit ist die Systemanmeldung der Unix-Rechner an AD angebunden – Zeit für ein erstes Resümee: Die NiS-AD-Administratoren müssen nur noch eine einheitliche Passwortdatenbank für Windows- wie Unix-Benutzer pflegen. Einzelne Client-Rechner erhalten keinen Zugriff mehr auf die kompletten Passwortdaten sämtlicher Benutzer, sondern verwenden zur Überprüfung der Identität einzelner Benutzer nun ein Challenge-Response-Verfahren zum Domänencontroller. Was sie bisher nicht überprüfen, ist die Identität des DC selbst. Der Sicherheitsgewinn hält sich somit in Grenzen, denn ein potenzieller Angreifer hat nach wie vor die Möglichkeit, etwa durch DNS-Spoofing, IP-Spoofing oder als Man-in-the-Middle dem Unix-Client einen präparierten Domänencontroller unterzuschieben und sich so Zugang zum System zu verschaffen. Um das zu verhindern, muss der Client der Domäne beitreten. Bei diesem Vorgang generiert der Administrator ein Computer-Passwort, das nur dem Client-Rechner und dem echten DC bekannt ist. Während der Systemanmeldung fordern Client-Rechner in einer Domäne dann nicht mehr nur ein initiales Ticket für den jeweiligen Benutzer an, sondern zusätzlich noch ein sogenanntes Host-Ticket, das der DC mit dem Computer-Passwort des Clients verschlüsselt. Der Client versucht, es mit seinem lokal hinterlegten Computer-Passwort zu entschlüsseln. Klappt das, kamen beide Tickets unverändert von einem authentischen Domänencontroller, und der Benutzer darf ins System.

Auf Windows-Rechnern genügt es, zum Domänenbeitritt den Namen eines administrativen Kontos samt Passwort einzugeben. Unter Unix gestaltet sich der Domänenbeitritt ohne Zusatzsoftware

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

wie Samba nicht ganz so einfach, da die zugehörige Netzkommunikation teilweise Microsoft-spezifische RPC-Aufrufe verwendet (siehe Kasten „Domänenbeitritt von Unix-Rechnern“). In jedem Fall aber kann der Administrator den Beitritt zur Domäne Schritt für Schritt von Hand durchführen. Dazu muss er zunächst auf dem Domänencontroller mit dem Verwaltungsprogramm „Active Directory Users and Computers“ ein Maschinenkonto für den Unix-Rechner anlegen. Das zugehörige Passwort ist zufällig gewürfelt und lässt sich weder vorgeben noch auslesen. Um es auf einen bekannten Wert zu ändern, setzt man am einfachsten mit einem weiteren Mausklick das Maschinenkonto zurück. Das Computer-Passwort entspricht dann schlicht dem Hostnamen des Rechners. Unter der Haube legt der Vorgang im KDC des AD einen neuen Principal für den Computer an, dessen Keys er aus dem Passwort ableitet. Allerdings unterscheiden sich zwischen Windows und Unix die Konventionen, wie die Namen von Computer-Principals auszusehen haben. Windows begnügt sich mit dem kurzen Rechnernamen.

Um zusätzlich auch einen Unix-konformen Namen im AD unterzubringen, bietet sich das Kommandozeilenwerkzeug *setspn* an. Microsoft liefert es aus als Teil der Support Tools zu Windows Server 2003, die auch kostenlos zum Download bereitstehen [b]. Mit *setspn -a host/linuxclient1.nis-ad.de linuxclient1* legt der Administrator im KDC einen zusätzlichen Host-Principal an, dessen Keys sich vom selben Passwort ableiten wie der ursprüngliche Maschinen-Principal „linuxclient1“. Die Unix-Welt erwartet, wie im Beispiel gezeigt, stets den vollqualifizierten DNS-Namen als Instanzteil des Host-Principals. Danach sind die Arbeiten auf Windows-Seite zunächst beendet.

Auf dem Unix-Rechner ändert der Administrator über das standardisierte *kpasswd*-Protokoll als Erstes das Maschinenpasswort vom voreingestellten Rechnernamen auf einen sicheren Wert. Das neue Passwort (in Listing 4: *yV]OLUN-I|W)* muss er daraufhin noch der Kerberos-Implementierung auf dem Unix-Rechner in Form einer *keytab*-Datei bekannt machen. Dazu nutzt er das bekannte Maschinenpasswort und generiert daraus dieselben Keys, wie sie im KDC hinterlegt sind. Welche Versionsnummer der KDC im AD aktuell für die Schlüssel des Rechners verwendet, erfährt er über das Kommando *kvno*. Die passenden Verschlüsselungstypen hängen von der eingesetzten Windows-Version des DC ab. Windows 2003 Server beispielsweise kennt „des-cbc-md5“ und „rc4-hmac“, die aktuelle Kerberos-Implementierungen unter Unix ebenfalls beherrschen. Listing 4 zeigt Schritt für Schritt die nicht ganz offensichtliche Prozedur am bereits erwähnten Beispiel des Linux-Rechners „linuxclient1.nis-ad.de“.

Teilziel erreicht: Sicherer Identitätsnachweis

Ist das erledigt, kann die Unix-Maschine während der Anmeldung nicht nur ein initiales Ticket für einen Benutzer anfordern, sondern damit im Anschluss auch ein weiteres Ticket für den eigenen Host-Principal. Passt das Ticket zur aktuellen Keytab, kommen die Antworten tatsächlich vom authentischen Domänencontroller. Einige Implementierungen des Moduls *pam_krb5* begnügen sich in den Standardeinstellungen allerdings damit, das initiale Ticket anzufordern und verzichten auf den zweiten Schritt, der die Echtheit des Absenders überprüft. Wer Wert auf sichere Authentisierung legt, sollte deshalb in jedem Fall die PAM-Konfiguration kontrollieren und gegebenenfalls über implementierungsabhängige Optionen wie „validate“ das Prüfen des Host-Tickets erzwingen.

Haben alle Unix-Rechner die nötigen Änderungen erfahren, ist Phase 1 des Migrationsprojektes bei NiS-AD abgeschlossen. Die Systeme werten die Passwort-Hashes der NIS-Map *passwd* nicht mehr aus, sie lassen sich durch Platzhaltereinträge ersetzen. Am Ziel sind die Administratoren jedoch längst noch nicht: Zwar muss jeder Benutzer nun mit einem sehr sicheren Verfahren seine Identität nachweisen, aber nach wie vor könnte ein Angreifer die NIS-Map *passwd* fälschen und einem gewöhnlichen Benutzer beispielsweise die User-Id 0 zuweisen und so Administrationsrechte erlangen. Damit das nicht mehr passieren kann, stellt die zweite Phase des Migrationsprojektes alle weiteren Benutzerinformationen für die Unix-Maschinen über AD zur Verfügung und sichert den Zugriff über kryptografische Methoden ab. Mit diesem Schritt wird sich der nächste Teil beschäftigen. (avr)

MARK PRÖHL,
MICHAEL WEISER

arbeiten bei der science + computing ag und sind als Consultants in den Bereichen Kerberos, LDAP und AD-Integration aktiv. Seit mehreren Jahren leiten Sie auch Trainingsveranstaltungen zu diesen Themen.

Literatur

[1] Joachim Keltsch, Mark Pröhl; Authentifizierung; Visumpflicht für alle; Kerberos wacht über Identität im Netz; *iX* 3/2007, S. 123





Listing 1: *krb5.conf*

```
[libdefaults]
     default_realm = NiS-AD.DE
[realms]
     NiS-AD.DE = {
          admin_server = dc1.nis-ad.de
          kdc = dc1.nis-ad.de
          kdc = dc2.nis-ad.de
          kdc = dc3.nis-ad.de
     }
```

Listing 2: *kinit*

```
admin@client1 % klist -5
klist: No credentials cache found (ticket cache
FILE:/tmp/krb5cc_1100_UzBtlP)
admin@client1 % kinit unixuser
Password for unixuser@NiS-AD.DE: ********
admin@client1 % klist -5
Ticket cache: FILE:/tmp/krb5cc_1100_UzBtlP
Default principal: unixuser@NiS-AD.DE
Valid starting     Expires            Service principal
07/28/08 14:56:22  07/29/08 00:56:24  krbtgt/NiS-AD.DE@NiS-AD.DE
```

Listing 3: PAM-Konfiguration

```
auth       sufficient   pam_krb5.so minimum_uid=1000 forwardable
auth       required     pam_unix.so nullok_secure use_first_pass
account    sufficient   pam_krb5.so minimum_uid=1000
account    required     pam_unix.so
session    optional     pam_krb5.so minimum_uid=1000
session    required     pam_unix.so
password   sufficient   pam_krb5.so minimum_uid=1000
password   required     pam_unix.so nullok obscure min=4 max=8 md5
```

Listing 4: Keytab

```
linuxclient1:~# kpasswd linuxclient1
Password for linuxclient1@NiS-AD.DE: linuxclient1
Enter new password: yVJOLUN-I|W
Enter it again: yVJOLUN-I|W
Password changed.
linuxclient1:~# kvno linuxclient1@NiS-AD.DE
linuxclient1@NiS-AD.DE: kvno = 4
linuxclient1:~# ktutil
ktutil: addent -password -p linuxclient1@NiS-AD.DE -k 4 -e rc4-hmac
Password for linuxclient1@NiS-AD.DE: yVJOLUN-I|W
ktutil: addent -password -p host/linuxclient1.nis-ad.de@NiS-AD.DE
                                                   -k 4 -e rc4-hmac
Password for host/linuxclient1.nis-ad.de@NiS-AD.DE: yVJOLUN-I|W
ktutil: wkt /etc/krb5.keytab
ktutil: quit
```

Onlinequellen

[a] *adtool*
gp2x.org/adtool/

[b] *ktpass.exe* (W2k3: Support Tools)
go.microsoft.com/fwlink/?LinkId=100114

[c] *msktutil*
download.systemimager.org/~finley/msktutil/

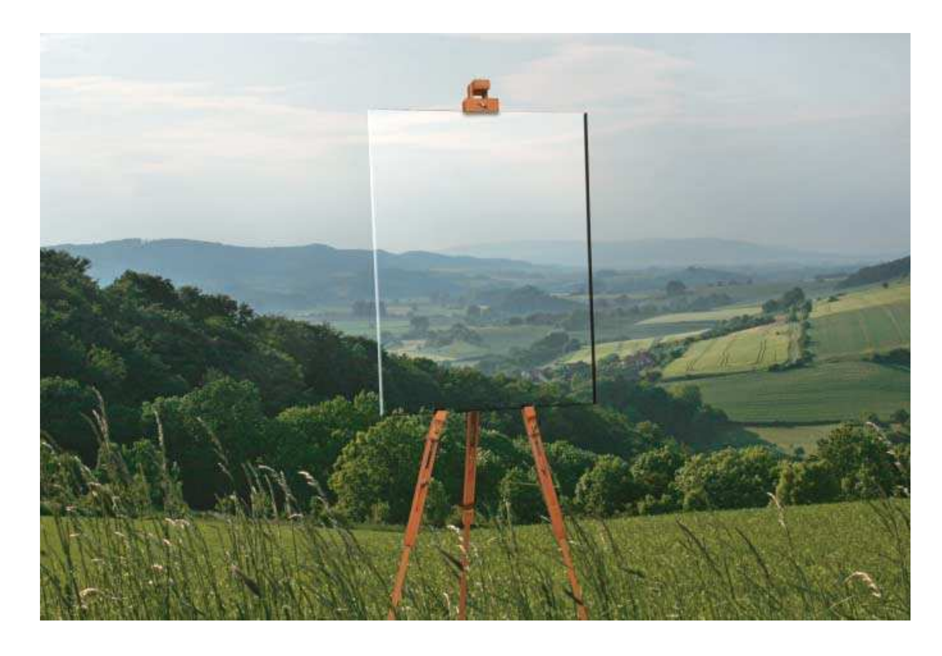
[d] *krb5servicetool*
sourceforge.net/projects/krb5servicetool

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

2D-Grafik mit *canvas* und Javascript

Weitblick

Tobias Günther



SVG ist für Grafiken im Web zu kompliziert und nicht alle Browser können damit umgehen. Für Flash und andere benötigen Browser ein Plug-in. Die in Arbeit befindliche Spezifikation des künftigen HTML beinhaltet das *canvas*-Element, das Entwickler per Javascript mit dynamischen Grafiken füllen können.

Javascript ist spätestens seit dem Web 2.0 über das „j" in Ajax als die Zutat bekannt, die für die Dynamik von Webseiten sorgt. Zusammen mit dem für HTML 5 vorgesehenen *canvas*-Element kann die Sprache dynamische Grafiken im Browser erstellen und manipulieren – ohne Flash- oder Java-Plug-in.

Dynamische Grafiken im Browser sind ein heikles Thema für jeden Web-Entwickler, denn es gibt nur eine Handvoll Optionen – und alle haben ihre Nachteile. Die klassische Variante ist, Grafiken nach alter Manier auf dem Server erstellen zu lassen oder vorzuhalten. Ajax-Programmierung kann das Erstellen anstoßen und die resultierende Grafik gleich wieder ins HTML-Dokument einbauen. Allerdings erfordert es zu viel Zeit, die Grafik zu erzeugen und zum Browser zu transferieren, als dass sie für dynamische Aufgaben taugten.

Flash, seit Jahren die wohl meistverwendete Variante, und seit Kurzem Silverlight heißen die Alternativen. Während diese Techniken in puncto Animation kaum zu schlagen sind, haben sie dennoch einige Nachteile: Bei Flash und Silverlight handelt es sich um Plug-ins (keine browsernativen Techniken), nicht offene Standards, und sie unterliegen lediglich der Kontrolle ihrer Hersteller Adobe und Microsoft. Besonders die lückenhafte Akzeptanz im B2B-Bereich und auf mobilen oder eingebetteten Geräten lässt über Alternativen nachdenken. Als Plug-ins sind die Inhalte zudem von der Struktur der eigentlichen HTML-Seite getrennt und schwerer zugänglich. Java kann dynamisch mit Grafiken arbeiten, läuft aber in einer eigenen Runtime und hat dieselben Nachteile wie die anderen Plug-ins.

canvas als Alternative im Browser

Eine Option für dynamische Grafiken im Browser bietet das *canvas*-Element. Es findet sich noch nicht in der aktuellen (X)HTML-Spezifikation, allerdings beschreibt es der Working Draft des kommenden HTML 5-Standards. Mittlerweile betreibt das W3C selbst die Entwicklung zu HTML 5, das ursprünglich von der Web Hypertext Application Technology Working Group (WHATWG) stammt.

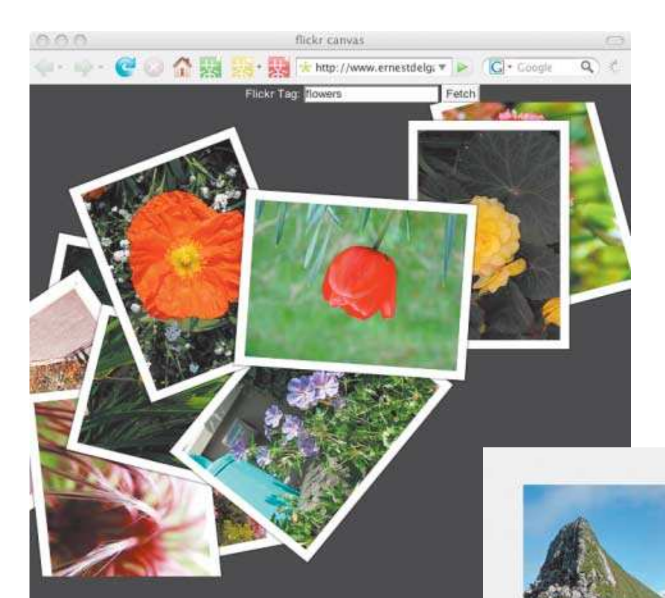
Die Geburt des *canvas* kam nicht nur spät, sondern wurde gleich kontrovers diskutiert: Apple erfand die Technik für das Dashboard seines Betriebssystems Mac OS X Tiger – und geriet dafür mächtig in die Kritik. Denn die Firma hatte damit den HTML-Standard „einfach so" erweitert, ohne den Weg über das World Wide Web Consortium (W3C) zu gehen und das Element zu standardisieren.

Warum Apple das neue Element erfand, lässt sich schnell erklären: Es gab zum damaligen Zeitpunkt keine vernünftigen Alternativen, Grafiken „on-the-fly" zu erstellen und zu manipulieren – ohne Plug-ins. SVG als Alternative wäre für die Aufgaben, die *canvas* erfüllt, zu komplex und umständlich gewesen. Dies hat sich bis heute nicht geändert. Deshalb und durch die durch Ajax gestiegene Beliebtheit von Javascript, das *canvas* manipulieren kann, erfreut sich das Element heute fast noch größerer Beliebtheit.

iX-TRACT

- Im Vorgriff auf das in Arbeit befindliche HTML 5 unterstützen Safari, Firefox und Opera das dafür vorgesehene Element *canvas* jetzt schon.
- Das Zeichnen von 2D-Grafiken, Spiegeln oder Rotieren von Bildern gestaltet sich ebenso einfach wie Verläufe oder Transparenz.
- Zur Unterstützung des Internet Explorer existiert eigens eine frei erhältliche Javascript-Brücke.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Ernest Delgado zeigt in seiner Anwendung [d] im Browser-Fenster drapierte Flickr-Fotos, die der Anwender verschieben und drehen kann (Abb. 2).

Durch einen Klick auf den Button kann der Surfer das Bild drehen (Abb. 3).

Da Apple *canvas* erfunden hat, wundert es wenig, dass Safari seit Version 2 als erster Browser das Element unterstützt. Allerdings fanden Mozilla (Firefox ab Version 1.5) und Opera (ab Version 9) schnell Gefallen daran und implementierten *canvas* in ihren Browsern. Microsofts Internet Explorer kennt bisher in keiner Version das neue Element – inklusive des kommenden IE8.

canvas wäre sicherlich dem Untergang geweiht, wenn es im Browser aus dem Hause Microsoft nicht nutzbar wäre. Glücklicherweise jedoch hatte der Entwickler Emil Eklund im Jahr 2005 ein paar freie Stunden und schrieb ein Javascript, das die *canvas*-Funktionen in Microsofts eigene Vector Markup Language (VML) umsetzt – die der Internet Explorer versteht. Google beschäftigt sich seither mit der Weiterentwicklung dieses Skripts und stellt es als *ExplorerCanvas* kostenlos zur Verfügung (siehe Onlinequellen [a]). Zwar funktionieren nicht sämtliche Features des *canvas* mit dem Skript, aber vieles ab IE 6 durchaus.



Spiegelung eines Bildes mit *canvas* sowie zunehmende Transparenz durch *globalCompositeOperation* (Abb. 1).

Bilder spiegeln und mehr

Was Entwickler mit *canvas* erreichen können, zeigen viele Websites der Web-2.0-Generation. Ein beliebter Effekt ist das Spiegeln von Bildern (siehe Abb. 1). Ein ähnlicher Effekt ist seit einiger Zeit ebenfalls häufig zu sehen: Die Ecke eines Bildes oder des Bildschirms (oft rechts oben) wird hochgeklappt gezeigt. Bewegt man die Maus über dieses Eselsohr, klappt die Ecke weiter zurück, und darunter verborgener, zusätzlicher Content (beispielsweise Werbung) kommt zum Vorschein.

Mit *canvas* vektorbasiert zu arbeiten, hat Yahoo in seiner Pipes-Applikation genutzt (siehe [b]). Die Bézierkurven, die zwei verknüpfte Container verbinden – und beim Verschieben per Drag & Drop immer flexibel bleiben –, sind mit *canvas* realisiert.

Die kleine Library MooWheel (siehe [c]), die auf der Opensource-Javascript-Bibliothek MooTools aufsetzt, nutzt ebenfalls Bézierkurven. Hiermit können Programmierer Verknüpfungen zwischen verschiedenen Objekten darstellen, beispielsweise für die Visualisierung eines Freundschaftsnetzes.

Eine interaktivere Anwendung ist das Fotoexperiment (siehe [d] und Abbildung 2) von Ernesto Delgado. Hier kann ein Benutzer einen Flickr-Tag eingeben und bekommt eine Auswahl

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 1: HTML-Code

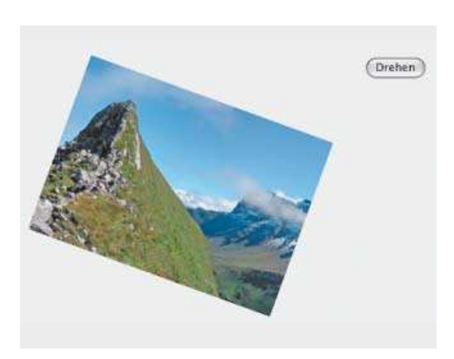
```
<html>
  <head>
    <!--[if IE]>
      <script type="text/javascript"
              src="excanvas.js"></script>
    <![endif]-->
    <script type="text/javascript"
            src="canvas.js"></script>
  </head>
  <body onload="init();">
    <canvas id="canvas" width="700" height="650"
            style="border:1px solid #f00;">
    </canvas>
    <button onclick="rotate_canvas(10);">Drehen</button>
  </body>
</html>
```

Listing 2: Initialfunktion

```
function init(){
  var image = new Image();
  image.src = "alpenpanorama.jpg";
  var canvas = document.getElementById('canvas');
  var kontext = canvas.getContext("2d");
  kontext.translate(350, 310)
  kontext.drawImage(image, 0, 0);
}
```

Listing 3: Drehen eines Objekts

```
function rotate_canvas(degrees){
  var rad = (Math.PI/180)*degrees;
  var canvas = document.getElementById('canvas');
  var kontext = canvas.getContext("2d");
  kontext.clearRect(0,0,700,650);
  kontext.rotate(rad);
  var image = new Image();
  image.src = "alpenpanorama.jpg";
  kontext.drawImage(image, 0, 0);
}
```



Listing 4: Pseudo-*iX*-Logo (Auszug)

```
// Linien zeichnen: "i"
kontext.beginPath();
kontext.moveTo(175,225);
kontext.lineTo(105,325);
<!-- ... -->
kontext.stroke();
// i-Punkt
kontext.arc(210, 180, 30, 0, Math.PI+(Math.PI*2)/2,
true);
kontext.fillStyle = "rgb(204, 204, 255)";
kontext.fill();
// "X" zeichnen
kontext.beginPath();
kontext.moveTo(235,225);
kontext.lineTo(135,365);
<!-- ... -->
kontext.lineTo(235,225);
kontext.fillStyle = "rgb(102, 102, 153)";
kontext.fill();
```

Die Methoden *translate* und *rotate* bewegen den Ursprung des Bildes in Abbildung 3 beziehungsweise drehen es um ihn herum (Abb. 4).

der gefundenen Fotos wie auf einem Fotoleuchttisch als Polaroids verstreut. Die Bilder lassen sich bewegen, skalieren und rotieren.

Ein anderer Einsatzbereich von *canvas* ist die Entwicklung browserbasierter Spiele. Von Tetris (siehe [e]) über ein einfaches Dungeon (siehe [f]) bis hin zu einem originalgetreuen Nachbau des Nintendo-Klassikers Super Mario World (siehe [g]) wurde *canvas* schon genutzt. Das zeigt, dass man selbst bei der Browser-Spieleentwicklung teilweise ohne Plug-ins arbeiten kann. Allerdings können solche Spiele nicht mit ihren Flash-Pendants mithalten – es geht hier eher um einen Proof of Concept mit dem Ziel, die Techniken in anderen Bereichen einzusetzen.

Wie *canvas* funktioniert

canvas ist ein Container für das dynamische Erstellen von Grafiken mit Javascript. Das bedeutet, dass Generierung und Manipulation live im Client über Javascript erfolgen. Das Element ähnelt in Funktion und Aussehen dem *img*-Element, hat jedoch kein *src*-Attribut für die Spezifizierung einer Bild-Quelle – da Javascript alle Manipulation am *canvas* durchführt.

Zunächst sei ein Bild in ein *canvas* importiert und anschließend um einige Grad gedreht – eine Funktion, die man mit CSS und HTML alleine nicht durchführen kann. Listing 1 zeigt das HTML-Gerüst. Damit der Internet Explorer „mitmachen“ kann, bindet ein *script*-Element das *ExplorerCanvas*-Javascript ein. Abgesehen davon enthält die Seite nur einen leeren *canvas*-Tag und einen Schaltknopf, der das Bild drehen soll.

Ein bisschen Applikationscode befindet sich in der Datei *canvas.js*. Nachdem der Browser das Laden des Dokuments im Browser abgeschlossen hat, führt er die Funktion *init* aus (siehe Listing 2).

Gleich in der ersten Zeile findet sich eine Besonderheit: Wie jede Manipulation muss das Importieren von Bildern über Javascript geschehen. Andere Wege wären, ein vorhandenes und geladenes Bild anzusprechen oder andere *canvas*-Elemente als Quelle zu benutzen.

Weiter in Listing 2 geht es damit, das im HTML (Listing 1) erstellte *canvas* per *getElementById* zu „holen“ und mit der Methode *getContext('2d')* zu initialisieren. Erst dadurch können Autoren überhaupt auf das *canvas*-Element zugreifen und es nutzen. Als einziger Parameter kommt momentan „2d“ infrage. Künftig soll außerdem ein 3D-Grafikkontext existieren.

Objekte mit *translate* und *rotate* drehen

Vor dem Einsetzen des Bildes in das *canvas* verschiebt die Methode *translate* den Ursprung der künftigen Aktionen auf einen anderen Punkt im Koordinatensystem. Die Funktion *drawImage* setzt das Bild ins *canvas*-Element ein. In der 3-Parameter-Variante der Methode sind das *image*-Objekt und die *x*- und *y*-Koordinaten anzugeben, auf denen das Bild im *canvas* platziert sein soll. Das in HTML 5 definierte *drawImage* erlaubt aber noch mehr: Mit zwei weiteren Parametern kann ein Autor die gewünschte Größe für das zu platzierende Bild einstellen. Vier weitere Parameter erlauben es, das Bild gleich zu beschneiden und nur einen Ausschnitt zu importieren.

Bis hierhin hätte ein gewöhnliches *img*-Element gereicht. Allerdings er-

Onlinequellen

[a]	ExplorerCanvas	excanvas.sourceforge.net/
[b]	Yahoo Pipes	pipes.yahoo.com
[c]	MooWheel	www.unwieldy.net/moowheel/
[d]	Canvas Photo Experiment	www.ernestdelgado.com/public-tests/canvasphoto/demo/flickr/flickr.html
[e]	Tetris	luismedel.com/labs/tetris/tetris.html
[f]	A Basic RayCaster	developer.mozilla.org/en/docs/A_Basic_RayCaster
[g]	Super Mario World	blog.nihilogic.dk/2008/04/super-mario-in-14kb-javascript.html
[h]	Saving canvas to image	www.nihilogic.dk/labs/canvas2image/
[i]	Opera 3D-Canvas	my.opera.com/timjoh/blog/index.dml/tag/canvas
[j]	Mozilla Canvas Tutorial	developer.mozilla.org/en/docs/Canvas_tutorial

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

laubt *canvas* unter anderem, Objekte zu drehen. Wenn im *canvas* mit Winkeln gearbeitet wird, werden diese stets im Bogenmaß oder Radiant angegeben. Wer lieber die geläufigeren Grade verwenden will, rechnet die Gradangabe ins Bogenmaß um (Listing 3).

Neu im Code-Snippet sind die Funktionen *clearRect* und *rotate*. Erstere legt einen Teil des *canvas* durch ein leeres Rechteck wieder frei. In Listing 3 löscht sie alle Zeichnungsobjekte von Koordinate 0/0 an. Ohne diesen Zwischenschritt würden die folgenden Aktionen übereinander zeichnen, was nicht beabsichtigt wäre. *rotate* dreht das *canvas* nun um den vorher mit *translate* definierten Mittelpunkt. Erst jetzt setzt *drawImage* wie vorhin das Bild ein.

Mit Grafikdateien zu arbeiten ist sicherlich ein spannendes Thema im Umgang mit dem *canvas*. Jedoch darf man die Vektorfunktionen nicht vergessen, die sich um das Zeichnen von Formen drehen: Gefüllte oder nur als Rahmen gezeichnete Rechtecke, Linien und Pfade, sowie Kreisformen und Bögen sind die elementaren Formen, die *canvas* erlaubt. Listing 4 enthält einen Auszug aus einem Skript, das eine Art *iX*-Logo darstellt – im Wesentlichen mit den Anweisungen *moveTo* und *lineTo*.

Weitere interessante Optionen ergeben sich durch Transparenz, Verläufe und Patterns. Mit Einschränkungen kann man sogar eine im *canvas* erstellte Komposition als Grafikdatei wandeln und speichern (siehe [h]). Dadurch, dass Javascript die bei der Manipulation des *canvas* verwendete Sprache ist, lassen sich Animationen ebenfalls realisieren – beispielsweise die Uhr im Dashboard von Mac OS X.

Fazit

Es bleibt abzuwarten, was der künftige 3D-Context umfasst. Opera hat schon erste Schritte in diese Richtung unternommen (siehe [i]). Schon jetzt ist *canvas* eine durchaus ernst zu nehmende und einsatzfähige Technik. Wer sich intensiver mit der Technik beschäftigen möchte, findet im Mozilla Developer Center (siehe [j]) ein umfangreiches Tutorial, das alle Grundlagen erklärt. (hb)

TOBIAS GÜNTHER

ist Geschäftsführer der Webagentur Puremedia in Stuttgart.





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Migration von Rich Clients auf die Rich Ajax Platform

Gemeinsam reich

Axel Böttcher, Martin Dilger

Die Eclipse Rich Client Platform ist eine etablierte Technik. In Kombination mit der Rich Ajax Platform bietet sie die Möglichkeit, Anwendungen mit grafischer Oberfläche und vielfältigen Interaktionsmöglichkeiten ins Web zu bringen – und zwar mit im Wesentlichen unverändertem Look & Feel.

Web- und Desktop-Applikationen auf einer gemeinsamen Plattform zu entwickeln und zu warten, vor allem auch eine akzeptable Wartbarkeit zu erzielen, ist ein Wunsch vieler Entwickler. Doch wollte der lange Zeit nicht recht in Erfüllung gehen. Denn bisher verfolgten die jeweiligen Toolkits besonders in Hinblick auf die Frontends komplett unterschiedliche Strategien: Im Web war man vor Ajax viel mit der Entwicklung von Templates für das Frontend beschäftigt, seien es Java Server Pages (JSP), Java Server Faces (JSF) oder Extensible Server Pages (XSP). Auf der Desktop-Seite dominieren die ereignisgetriebenen Komponenten-Toolkits in Form des Abstract Window Toolkit (AWT), Swing und schließlich das Standard Widget Toolkit (SWT), die als Java-API angeboten werden. Eine Annäherung beider Welten wurde stets betrieben, aber erst Ajax hat ganz neue Möglichkeiten für die Gestaltung von Web-Frontends eröffnet. Doch auch Frameworks wie ZK, Echo2 oder das Google Web Toolkit (GWT) erlauben nur eine eingeschränkte Wiederverwendung von Frontend-Code für eine reine Client-Applikation.

Kein Ansatz ging bisher so weit wie die Eclipse-Plattform mit ihren beiden Ausprägungen „Rich Client Platform“ (RCP) und „Rich Ajax Platform“ (RAP): Ohne großen Mehraufwand können Programmierer Rich Clients für den Desktop und parallel für das Web entwickeln. RAP führt kein neues Programmierkonzept ein, sondern adaptiert die etablierten und gut dokumentierten Konzepte der Eclipse RCP für die Entwicklung von Webanwendungen.

Ähnlichkeiten in den Architekturen

Prinzipiell folgt die Architektur der Rich Ajax Platform der der RCP, deren Komponenten jedoch teilweise für RAP reimplementiert wurden. Die Applikationslogik einer Rich-Ajax-Anwendung wird auf Serverseite ausgeführt. Als Ablaufumgebung kommt wie gewohnt die OSGi-Implementierung der Eclipse-Plattform (Equinox) zum Einsatz. Zur Darstellung der Benutzeroberfläche auf der Client-Seite dient Qooxdoo, ein Open-Source-Framework für Javascript. Den Javascript-Code für die Benutzeroberfläche generiert die Rich Ajax Platform dynamisch zur Laufzeit.

Zum großen Teil wurde das Funktionsspektrum des SWT für die Rich Ajax Platform reimplementiert, es steht unter der Bezeichnung RWT (RAP Widget Toolkit) zur Verfügung. Bisher hat man aber nicht alle Funktionen aus dem SWT für den Einsatz in der Rich Ajax Platform umgesetzt, beispielsweise sind einige Mouse Events nicht verwendbar. Die fehlende Umsetzung bestimmter Funktionen hat einerseits technische Gründe, weil diese nicht (oder zumindest nicht in der im SWT gewohnten Form) für den Einsatz in einer Webumgebung geeignet sind. In einigen Fällen hat man die Implementierung einfach aus zeitlichen Gründen auf spätere Versionen verschoben.

Die angesprochenen Mouse Events dürften in die erste Kategorie fallen: Zur Übertragung der exakten Bewegungen der Maus (für *MouseMove-*

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Events) wären riesige Datenmengen zu übertragen, was inkonsistentes Verhalten oder starke Verzögerungen aufgrund von Latenzzeiten zur Folge haben könnte. Einfache Ereignisse wie Klicks, Doppelklicks oder das Öffnen von Kontextmenüs sind von dieser Einschränkung nicht betroffen und im RWT entsprechend umgesetzt.

Aufgrund der unterschiedlichen Laufzeitumgebung bietet das RWT im Vergleich zum SWT hingegen einige Ergänzungen, unter anderem eine erweiterte Event-Verarbeitung für die Client-Server-Umgebung, Zugriff auf die Javascript-Komponenten der Benutzeroberfläche sowie die Synchronisierung von clientseitiger Benutzeroberfläche und serverseitiger Applikation.

Sessions teilen sich eine Instanz

Bedingt durch die kleinen Unterschiede in den Architekturen unterscheidet sich die Implementierung einer RAP-Anwendung leicht von der einer RCP-Anwendung, wie das folgende Beispiel zeigt.

Im Gegensatz zu RCP können innerhalb einer RAP-Anwendung mehrere Benutzersessions auf eine Applikationsinstanz zugreifen. Zur Laufzeit lassen sich deshalb die für Webapplikationen üblichen Gültigkeitsbereiche ausmachen:

– Application Scope: Gültigkeitsbereich, in dem alle Benutzersessions auf die gleichen Objekte zugreifen; erstreckt sich vom Startzeitpunkt einer Anwendung bis zu ihrer Beendigung. Dieser Bereich entspricht dem, der in der Rich Client Platform vorhanden ist.

– Session Scope: Gültigkeitsbereich, in dem die Daten sessionbasiert zur Verfügung stehen. Sessions sind erforderlich, weil die Kommunikation zwischen Client und Server über das zustandslose HTTP-Protokoll erfolgt.

– Request Scope: Gültigkeitsbereich, der während der Verarbeitung einer einzelnen Anfrage aktiv ist.

Da für den Zugriff auf eine RAP-Applikation nicht wie bei der RCP für jeden Benutzer beziehungsweise jede Session eine neue Applikationsinstanz gestartet wird, unterscheidet sich die Implementierung des Einstiegspunktes für die Applikation in beiden Plattformen. In der Rich Client Platform wird hierfür eine Implementierung des Interface *IApplication* und der Methode *start(IApplicationContext context)* erwartet. Die Rich Ajax Platform hingegen verlangt eine Implementierung des Interface *IEntryPoint* mit der Methode *createUI()*. Diese Methode arbeitet die Rich Ajax Platform für jeden Benutzer beim Start einer Benutzersession ab. Die *IEntryPoint*-Implementierung wird über den Extension-Point *org.eclipse.rap.ui.entrypoint* bei der Plattform registriert. Eine beispielhafte Implementierung zeigt das folgende Code-Fragment:

```
public int createUI() {
   Display display = PlatformUI.createDisplay();
   int result = PlatformUI.createAndRunWorkbench ↵
      (display, new ApplicationWorkbenchAdvisor());
   return result;
}
```

Statische Elemente und somit auch Instanzen von Klassen, die nach dem Singleton-Pattern implementiert sind, werden von allen Benutzersessions gleichzeitig genutzt und befinden sich im Application Scope. Eine gemeinsame Verwendung ist jedoch in bestimmten Fällen nicht erwünscht. Die Rich Ajax Platform bietet aus diesem Grund die Möglichkeit, Singletons sessionbasiert zur Verfügung zu stellen. Hierfür erfolgt eine Ableitung von der abstrakten Klasse *SessionSingletonBase* aus dem Paket *org.eclipse.rap.rwt*. Diese Klasse bietet die Methode *getInstance (Class type)*, über die der Entwickler jeweils eine eigene Instanz der Klasse für jede Benutzersession zur Verfügung stellen kann. Der Parameter *type* gibt

iX-TRACT

- Viele Oberflächenelemente der Rich Client Platform (RCP) und der Rich Ajax Platform (RAP) – beides Eclipse-Plug-ins – entsprechen sich, sodass sich eine Anwendung von der einen auf die andere Plattform relativ leicht migrieren lässt.
- Programmierer können Desktop- und Webanwendungen parallel entwickeln und dabei einen Großteil des Quellcodes wechselseitig wiederverwenden.
- Plattformspezifische Elemente lassen sich in entsprechende Plug-ins auslagern, die eine Anwendung nach Bedarf lädt.

RAP in der Praxis

Um Eclipse als Rich Ajax Platform nutzen zu können, muss diese Target-Plattform zunächst installiert werden. Das bewerkstelligt man am einfachsten per Update-Mechanismus über die Update-Site. Nach dem Download und dem obligatorischen Neustart von Eclipse fordert die IDE zur Installation der Zielplattform auf. Mit Eclipse lassen sich nun Plug-ins für die beiden unterschiedlichen Plattformen RCP und RAP bauen, allerdings nicht für beide gleichzeitig. Die Zielplattform für die Plug-ins lässt sich über die Preferences umschalten und zwar unter „Plug-in->Target Platform“. Anschließend kompiliert Eclipse die Plug-ins gegen das gewählte Target.

Die Plug-ins haben in beiden Plattformen den gleichen Namen. Daher dürfen die der RAP keinesfalls in das Plug-in-Verzeichnis der Eclipse-Installation kopiert werden, weil das Überschreiben das lauffähige Eclipse zerstören würde – auch wenn ein Großteil der Plug-ins in beiden Plattformen identisch ist.

Nach dem Umschalten werden bei den Plug-ins für die jeweils nicht verwendete Plattform Syntaxfehler angezeigt. Es empfiehlt sich daher, separate Workspaces zu verwenden. Gemeinsam genutzte Bundles kann der Anwender entweder direkt als fertige Plug-ins einbinden oder in beide Workspaces importieren.

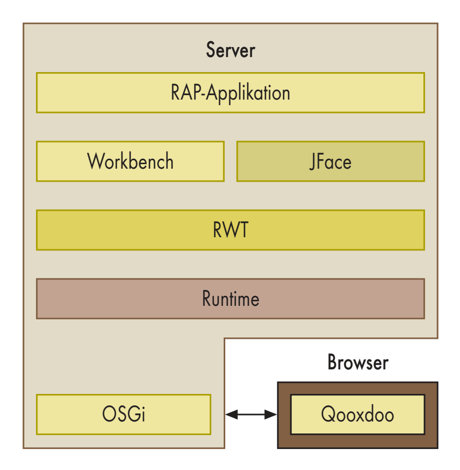
Will man UI-Plug-ins in beiden Plattformen verwenden, kann man die Abhängigkeiten im Manifest mit dem Zusatz *resolution:=optional* kennzeichnen. Dann lässt sich die Struktur für beide Plattformen mithilfe eines Manifests beschreiben. Beispielsweise lädt die Angabe

```
Require-Bundle: org.eclipse.ui;
resolution:=optional,org.eclipse.rap.ui;
resolution:=optional,org.eclipse.core.runtime,
```

stets das korrekte UI-Plug-in. Die Launch-Konfiguration startet RAP-Anwendungen über den Typ „RAP Application“. Bei der Auswahl der zu ladenden Plug-ins muss der Anwender im zugehörigen Reiter die Bundles *org.eclipse.rap.demo* deaktivieren, da Eclipse sonst die Demo-Anwendung der Plattform startet, was verwirrend sein kann. Beim Start der RAP-Anwendung stellt die IDE die Benutzeroberfläche automatisch im integrierten Webbrowser dar.

Ein Hinweis zum Debugging: Beim Start der RAP erscheint automatisch die OSGi-Konsole. Treten während der Ausführung Probleme auf, kann man sich alle aktuell geladenen Bundles mit dem Befehl *osgi> ss* anzeigen lassen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Die Architektur der Rich Ajax Platform unterscheidet sich kaum von der der Rich Client Platform (Abb. 1).

hierbei den Typ des Objekts an. Beim ersten Aufruf der Methode innerhalb einer Benutzersession wird eine Instanz dieses Typs in der aktuellen Session gespeichert und steht fortan für deren Dauer zur Verfügung. Diesen Mechanismus verwendet die Rich Ajax Platform intern, um beispielsweise die Workbench sessionbasiert zur Verfügung zu stellen.

Server versendet Nachrichten

Der prinzipielle Mechanismus für den Zugriff auf eine Webseite ist, dass ein Client eine Anfrage an den Webserver sendet. Dieser bearbeitet den Request, führt die nötigen Berechnungen durch und sendet eine Antwort mit der angeforderten Seite an den Client zurück. Während der Server die nötigen Berechnungen durchführt, wartet der Client auf dessen Antwort. Durch den Einsatz von Ajax wird die Wartezeit zwischen Anfrage und Antwort umgangen, was ein flüssiges Arbeiten ermöglicht. Der Austausch der benötigten Daten geschieht asynchron im Hintergrund, ohne dass der Benutzer dies wahrnimmt.

Ein *UICallback*-Mechanismus verlangt das Senden von Nachrichten vom Server an einen bestimmten Client. Um Nachrichten vom Server an einen Client schicken zu können, muss dieser Client dem Server über eine einzelne Anfrage hinaus bekannt sein. Dies ist in einer HTTP-basierten Webumgebung nicht gegeben. Ein Beispiel für die Notwendigkeit dieses Mechanismus ist die Aktualisierung der Benutzeroberfläche aus serverseitigen Threads. Da sich die Threads auf der Serverseite befinden, können sie nicht ohne Weiteres Nachrichten an bestimmte Clients senden. Der *UICallback*-Mechanismus kann über die statischen Methoden *activate(String ID)* und *deactivate(String ID)* der Klasse *UICallback* aktiviert beziehungsweise deaktiviert werden. Die Aktivierung des Mechanismus blockiert eine Client-Anfrage auf dem Server. Besteht die Notwendigkeit, eine Nachricht vom Server an einen Client zu senden, verarbeitet der Server die blockierte Anfrage und sendet die Antwort.

Grundsätzlich ist dieser Mechanismus deaktiviert. Sollen UI-Callbacks innerhalb der gesamten Anwendung zur Verfügung stehen, kann der Mechanismus direkt in der Implementierung der *createUI()*-Methode des *IEntryPoint*-Interface aktiviert werden.

Die Daten einer Session lassen sich durch den Aufruf der Methode *RWT.getSessionStore().setAttribute(String name, Object value)* setzen und durch *RWT.getSessionStore().getAttribute(String name)* wieder auslesen. Der direkte Zugriff auf die Sessiondaten ist aber nur während der Verarbeitung einer Client-Anfrage (Request Scope) möglich. Ist es nötig, dass der Server außerhalb dieses Gültigkeitsbereichs auf die Daten einer Session zugreift, muss er sie bereits zuvor aus der Session geladen und für die spätere Verwendung zwischengespeichert haben.

Eine Alternative besteht darin, auf die Sessiondaten über die statische Methode *runNonUIThreadWithFakeContext(Display display, Runnable runnable)* der Klasse *UICallback* zuzugreifen. Diese Methode erwartet als ersten Parameter ein Objekt vom Typ *Display* und als zweiten eins vom Typ *Runnable*. Innerhalb dieser Methode wird eine Client-Anfrage simuliert, wodurch der Zugriff auf die Sessiondaten aus dem übergebenen *Runnable* auch außerhalb des Request Scope ermöglicht wird.

Jede Benutzersession hat genau eine gültige *Display*-Instanz, die in der zuvor beschriebenen *IEntrypoint*-Implementierung erzeugt wird. Da diese ebenfalls in der Session gespeichert ist, muss der Client sie rechtzeitig zu einem geeigneten Zeitpunkt aus der Session laden und für die spätere Verwendung zwischenspeichern.

Gemeinsame IDE für RCP und RAP

Ein großer Vorteil der Rich Ajax Platform besteht darin, dass sie auf denselben Konzepten wie die Rich Client Platform beruht. Aus diesem Grund kann man eine RCP-Applikation ohne aufwendiges Refactoring und unter Wiederverwendung eines Großteils des entwickelten Sourcecodes auf die Rich Ajax Platform migrieren. Damit dies möglichst effektiv geschieht, sollte man einige Details im Design der Software beachten.

Verwendet ein Programmierer innerhalb eines Plug-in plattformspezifische Funktionen, muss er es für die Verwendung in beiden Plattformen in ein Basis-Plug-in und jeweils ein plattformspezifisches untergliedern. Das

Unterschiede zwischen RCP und RAP

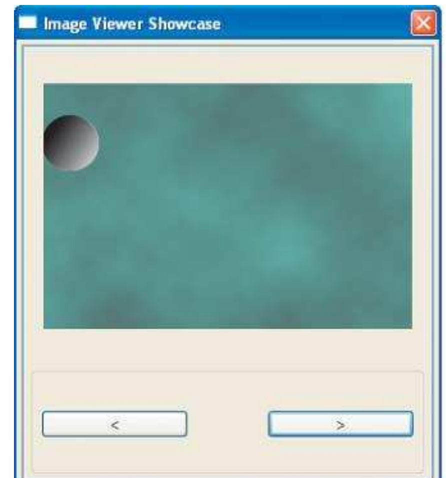
	Rich Client Platform (RCP)	Rich Ajax Platform (RAP)
Klasse für den Einsprung	Muss *IApplication* implementieren, dort die Methoden *start(IapplicationContext context)* sowie *stop()*.	Muss *IEntryPoint* implementieren. Achtung: Seit Version 1.1M2 liefert die Methode *createUI()* einen Integer-Wert zurück und nicht mehr eine Instanz von *Display*.
Extension Point zur Registrierung	*org.eclipse.core.runtime.applications*	*org.eclipse.rap.ui.entrypoint*
Zugriff auf lokales Dateisystem des Client	möglich (z. B. über *org.eclipse.core.filesystem* oder die Java-File-API)	nicht möglich
User Interface	Alle Funktionen und Widgets im SWT vorhanden.	Im RWT sind nicht alle SWT Widgets und Funktionen adaptiert, z. B. keine *MouseMotionListener*.
Ressourcen-Verwaltung (etwa *Fonts*, *Colors* und *Images*)	Können direkt instanziiert werden (*new*-Operator).	Werden unter allen Benutzersessions geteilt. Das Laden von Instanzen erfolgt über die Klasse *org.eclipse.rwt.graphics.Graphics*. Ressourcen (z. B. *Image*-Dateien) müssen sich im *Classpath* der Anwendung befinden.

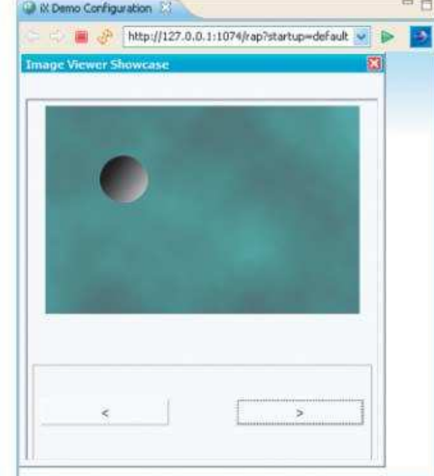
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Basis-Plug-in enthält die Funktionen, die ohne Veränderung in beiden Plattformen nutzbar sind. In den plattformspezifischen Plug-ins hingegen befinden sich die Funktionen, die sich in ihrer Implementierung in den beiden Plattformen unterscheiden.

Plattformspezifische Unterschiede

Für welche Implementierungen dies zutrifft, muss der Entwickler Plug-in-spezifisch überprüfen. Wichtige Indikatoren sind unter anderem:
– Unterschiedliche Anforderungen: Das Funktionsspektrum für beide Plattformen unterscheidet sich bereits in der Anforderung. Beispielsweise ist denkbar, dass die Applikation über eine Weboberfläche kein Editieren von Daten ermöglichen soll, was eine separate Implementierung der Benutzeroberfläche notwendig macht.
– Unterschiedliche Implementierung: Die Applikation unterscheidet sich in der Implementierung. Dies ist beispielsweise beim Einsatz sessionbasierter Singletons der Fall, die jeweils eine andere Umsetzung erfordern.
– Unterschiedliches Funktionsspektrum: Plattformspezifische Funktionen stehen in der jeweils anderen Plattform nicht zur Verfügung, beispielsweise wenn für die Rich Ajax Platform eine eigene Komponente implementiert wurde, die die Rich Client Platform nicht verwenden kann.





Die Beispielapplikation erscheint in der RCP (links) nur unwesentlich anders als in der RAP (rechts) (Abb. 2).

Als kleines Beispielprojekt soll ein Image Viewer dienen, der über zwei Buttons das Blättern durch Fotos ermöglicht. (Die Quelltexte sind wie üblich über den *iX*-Listingserver verfügbar.) Um das Programm übersichtlich


Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 1

```
private File[] fileList;
    /** current index of the image. */
    private int index = 0;
    /** Custom Constructor, used to load all images
        from the provided resource-plugin.
    */
    public ImageLoader() {
        Bundle bundle = Platform.
         getBundle(Activator.RESOURCES_PLUGIN_ID);

        try {
            URL url = FileLocator.toFileURL(bundle.
               getEntry("images"));
            File f = new File(url.getFile());
            fileList = f.listFiles();

        } catch (IOException e) {
            System.out.println("Error Loading Images.");
            e.printStackTrace();
        }

    }
private Image loadImage(String key) {
        try{
        Image im = Graphics.getImage(key,
         new FileInputStream(fileList[index]));
        return im;
        }catch(FileNotFoundException fnfex){
            System.out.println("Error, image " + key +
             " could not be loaded.");
            fnfex.printStackTrace();
        }
        return null;
    }
```

Der Image Loader für die Rich Ajax Platform verwendet die Klasse *Graphics*, um Ressourcen zu laden.

Listing 2

```
private Image loadImage(String key) {
       Image im = registry.get(key);
       if (im == null) {
           im = new Image(Display.getCurrent(),
                   fileList[index].getAbsolutePath());
           registry.put(fileList[index].getName(), im);
       }
       return im;
}
```

Der Image Loader für die Rich Client Platform verwendet eine JFace-Imageregistry, weil hierdurch das „Aufräumen“ der Ressourcen automatisch erfolgt.

zu gestalten, wurden Aspekte wie Logging und Fehlerbehandlung möglichst einfach implementiert.

Das Beispiel nutzt ausschließlich UI-Komponenten, die in beiden Plattformen vorhanden sind. Die Implementierung eines Plug-in für die Benutzeroberfläche erfolgt wie im Eclipse-SWT gewohnt. Das Plug-in lässt sich ohne Anpassung in beiden Umgebungen verwenden. Auf Knopfdruck soll die Anwendung Bilder laden und darstellen. In der Rich Client Platform kann dies einfach durch Zugriff auf das Dateisystem erfolgen. Auf der RAP ist das Arbeiten mit Ressourcen komplizierter, weil mehrere Benutzersessions gleichzeitig darauf zugreifen können. Daher sind zwei unterschiedliche Implementierungen erforderlich. Dazu kehrt ein Interface für das Laden der Bilder zunächst die Abhängigkeiten um (eine Anwendung des Dependency Inversion Principle [1]), sodass das Basis-Plug-in nicht mehr vom Plug-in abhängig ist, das die Klasse *ImageLoader* zur Verfügung stellt, sondern umgekehrt:

```
package sample.ix.image;
import org.eclipse.swt.graphics.Image;
public interface IImageLoader {
   public Image getNextImage();
   public Image getPreviousImage();
}
```

Diese Schnittstelle kapselt ein neuer Extension Point *ix.sample.imageViewer*, bei dem eine Implementierung des *IImageViewer*-Interface registriert werden kann. Für jede Plattform stellt ein plattformspezifisches Plug-in eine Implementierung des Interface zur Verfügung und registriert sie über eine Extension. Zur Laufzeit steht dann je nach geladenem Plug-in die benötigte Implementierung zur Verfügung.

Die *Activator*-Klasse jedes dieser Plug-ins schließlich lädt den konkreten plattformspezifischen *ImageLoader* aus dem Extension-Point. Zur Demonstration wurde der Code hierfür für beide Plattformen dupliziert. Hier bietet sich ein Refactoring an, unter Einsatz eines Dependency Injection Framework, etwa Spring oder Google-Guice. Das Beispiel implementiert keine weitere Business-Logik. Diese müsste man genauso, wie eben demonstriert, von den plattformspezifischen Bestandteilen trennen.

Fazit

Die Rich Ajax Platform stellt in der aktuellen Version 1.1 eine einsatzfähige Plattform zur Entwicklung von Ajax-Anwendungen dar. Für versierte Eclipse-RCP-Entwickler hält sich der Einarbeitungsaufwand zudem in Grenzen, weil die Konzepte und Vorgehensweisen in weiten Bereichen identisch sind. Die Synergien zwischen den beiden Plattformen sorgen für eine breite gemeinsame Codebasis und vereinfachen die Entwicklung für beide Plattformen erheblich.

Noch fern ist jedoch die Vision eines „Write Once, Run On Desktop and Web“. Zu unterschiedlich sind die Voraussetzungen, die die Synchronisierung von Client und Server im Web im Vergleich zur reinen Desktop-Anwendung mit sich bringt. Um eine hohe, plattformübergreifende Wiederverwendbarkeit zu erreichen, muss der Entwickler im Design bereits weitgehend Rücksicht auf die Unterschiede nehmen.

Die Migration von einer Plattform auf die andere ist ebenfalls mit einigem Zusatzaufwand verbunden, durch die verwandten Plattformen aber auf jeden Fall einfacher und effizienter zu erreichen als mit anderen Techniken. Es spielt dabei keine Rolle, ob von RCP auf RAP oder anders herum migriert wird, auch wenn Ersteres aufgrund der Verbreitung der Rich Client Platform das weitaus häufigere Einsatzszenario darstellen dürfte. (ka)

MARTIN DILGER

arbeitet als Consultant bei der Pentasys AG in München.

DR. AXEL BÖTTCHER

ist Professor für Informatik an der Hochschule München. Er beschäftigt sich mit Softwarearchitektur und agilen Methoden.

Onlinequellen

Homepage der Rich Ajax Platform	www.eclipse.org/rap/
Eclipse RAP Updatesite	download.eclipse.org/technology/rap/update-site
RAP-Blog	rapblog.innoopract.com
Qooxdoo Framework	qooxdoo.org
Google Guice	code.google.com/p/google-guice/
Beispielprogramm des Artikels	ftp://ftp.heise.de/pub/ix/ix_listings/2008/10

Literatur

[1] Robert C. Martin; Agile Software Development; Principles, Patterns, and Practices; Prentice Hall 2002





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Silverlight-2-Tutorial, Teil III: Flickr-Slideshow und Videos

Im Strom

Regina Dowling, Jörg Müller

Der letzte Teil des Silverlight-Tutorials baut das digitale Fotoalbum aus dem zweiten Teil zu einer einfachen Slideshow mit Flickr-Anbindung aus. Außerdem gibt er einen Einblick in die Videofähigkeiten der Webplattform und den Silverlight-Streaming-Dienst von Microsoft.

Will man digitale Bilder mit anderen teilen oder archivieren, hat man die Wahl zwischen mehreren etablierten Webdiensten, von denen einige eine API zum Einbinden der Bilder in eigene Anwendungen anbieten. Der dritte Teil des Tutorials soll das einfache Fotoalbum aus der letzten Ausgabe so erweitern, dass die Anwendung Bilddaten über die Schnittstelle von Flickr lädt. Um ein eigenes Flickr-Konto nicht zur Voraussetzung zu machen, werden lediglich die öffentlichen Daten der Plattform angezapft. Per Drag & Drop kann man dann eine Auswahl davon zu einer einfachen Slideshow zusammenstellen.

Wiederum wird das Aussehen der Anwendung hauptsächlich in der Datei *Page.xaml* festgelegt. Neben dem Hintergrund und dem grundsätzlichen Layout-Grid definiert die Datei die folgenden Bereiche:

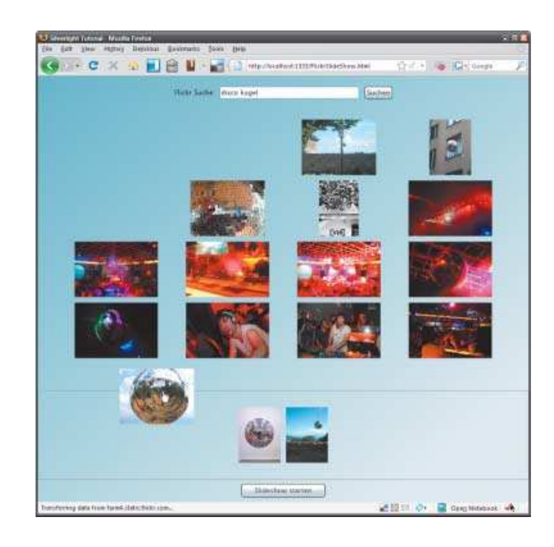
– UI-Controls zur Eingabe des Suchbegriffs,
– eine Übersicht der geladenen Bilder (in Tabellenform als Grid implementiert),
– ein *Image*-Control zur Anzeige der Slideshow, mit Storyboards zum Ein- und Ausblenden des Bildes,
– eine scrollbare Bilderleiste für die Thumbnails der ausgewählten Bilder (wie schon im Album wird dazu ein horizontales *StackPanel* innerhalb eines *ScrollView*-Control verwendet),
– ein Button zum Umschalten zwischen Übersicht und Slideshow, der nur sichtbar sein soll, wenn der Anwender mindestens ein Bild ausgewählt hat.

Das XAML-Markup, das die Oberfläche der Suche definiert, enthält ein paar neue Controls: einen *TextBlock* zur Beschriftung, das Eingabefeld (*TextBox*) und einen *Button* zum Absenden der Daten (Listing 1). Letzterer ist mit dem Eventhandler *searchButton_Click* verknüpft, der über *loadImages* die eigentliche API-Methode aufruft.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 1: Benutzer-Interface für die Suche in *Page.xaml*

```
<StackPanel x:Name="searchControl" Grid.Row="1" Grid.Column="1"
   Orientation="Horizontal" HorizontalAlignment="Center"
    VerticalAlignment="Center" >
    <TextBlock x:Name="searchInputLabel"
           Text="Flickr Suche: "FontSize="12" FontFamily="Tahoma"
           Height="22" Padding="0, 2, 5, 0" />
    <TextBox x:Name="searchInput" Text="Bitte Suchbegriff eingeben..."
            FontFamily="Tahoma" FontSize="12"
            Padding="2" Width="250" Height="22"/>
    <Button x:Name="searchButton" Content="Suchen" FontFamily="Tahoma"
            FontSize="12"  Click="searchButton_Click" Margin="10, 0, 0, 0" Height="22"/>
</StackPanel>
```



Die Drag&Drop-Funktion muss der Anwender selbst implementieren (Abb. 1).

Den REST-Service von Flickr spricht die Anwendung über eine Instanz der Klasse *WebService* an. Als Ergänzung zur Basis-URL übergibt sie sowohl den API-Key als auch den Suchstring (aus dem Eingabefeld *searchInput*) als Teil des Querystring. Nach dem Empfang der (asynchron) geladenen Daten löst sie den Web-Client-Event *DownloadStringCompleted* aus und verarbeitet ihn im zugehörigen Handler *flickrService_DownloadStringCompleted* (Listing 2).

Anfordern der Bilder per Webservice

Der Service gibt eine XML-kodierte Liste von Bildern zu dem gesuchten Text zurück (Listing 3). Diese XML-Daten können dank der *LinqToXml*-Unterstützung in Silverlight 2 einfach weiterverarbeitet werden. Da *LinqToXml* allerdings nicht Teil der Grundfunktionen ist, muss man dem Projekt in Visual Studio eine Referenz auf *System.Xml.linq.dll* hinzufügen (im Solution Explorer: Rechtsklick auf „References > Add Reference > System.Xml.linq.dll“).

Eine Klasse *FlickrImage* (Listing 4) soll die wichtigsten Eigenschaften jedes Bildes speichern, damit die Anwendung die URL zur entsprechenden Datei auf den Flickr-Servern konstruieren kann. Dazu gehören:

– die ID des Bildes (*Id*),
– ein Zugangscode (*Secret*),
– der Server (*Server*)
– sowie die Server-Farm (*Farm*).

Der zusammengesetzte Pfad ist später über das Attribut *ImageUrl* abrufbar. Die Beispielanwendung zeigt die ersten 16 Bilder der resultierenden Liste als Thumbnails in einer 4-x-4-Tabelle an.

Per Drag & Drop lassen sich die Bilder, die als Slideshow angezeigt werden sollen, in den unteren Bildschirmbereich ziehen (Abbildung 1). Dort erscheinen die Thumbnails in einer horizontalen Bilderleiste, durch die der Anwender bei

Listing 2: Aufruf des Flickr-Webservice

```
void loadImages(string topic)
{
    string apiKey = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";
    // bitte eigenen API-Key anfordern!
    string flickrUrl = String.Format("http://api.flickr.com/services/rest/?method=flickr.photos.search&api_key={1}&text={0}",
                                                                                                        topic, apiKey);
    WebClient flickrService = new WebClient();
    flickrService.DownloadStringCompleted += new DownloadStringCompletedEventHandler(flickrService_DownloadStringCompleted);
    flickrService.DownloadStringAsync(new Uri(flickrUrl));
    searchInput.Text = "Bilder werden geladen...";
}
```

Listing 3: Beispielantwort des Flickr-Webservice im XML-Format

```
<?xml version="1.0" encoding="utf-8" ?>
<rsp stat="ok">
  <photos page="1" pages="324" perpage="100" total="32349">
    <photo id="xxxxxxxxxx" owner="xxxxxxxxxxxx" secret="xxxxxxxxxx" server="xxxx" farm="x" title="xyz" ispublic="1" isfriend="0"
                                                                                                        isfamily="0" />
    <photo id="xxxxxxxxxx" owner="xxxxxxxxxxxx" secret="xxxxxxxxxx" server="xxxx" farm="x" title="xyz" ispublic="1" isfriend="0"
                                                                                                        isfamily="0" />
    ...
  </photos>
</rsp>
```

Listing 4: Klasse *FlickrImage.cs*

```
public class FlickrImage
{
    public string Id { get; set; }
    public string Secret { get; set; }
    public string Server { get; set; }
    public string Farm { get; set; }
    public string ImageUrl
    {
        get
        {
            return string.Format("http://farm{0}.static.flickr.com/{1}/{2}_{3}.jpg",
                Farm, Server, Id, Secret);
        }
    }
}
```

iX-TRACT

- Durch Nutzung der Flickr-API kann eine Silverlight-Anwendung öffentliche oder eigene Bilder zu einer Slideshow kombinieren.
- Videos in Microsofts WMV-Format lassen sich über ein Silverlight-Control relativ einfach in Anwendungen einbinden und abspielen.
- Mit dem Service Silverlight Streaming (SLS), über den Benutzer eigene Anwendungen und Videos kostenlos im Web veröffentlichen können, will Microsoft seine neue Technik fördern.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Bedarf scrollen kann. Das eingesetzte „Ziehen und Ablegen“ ist nicht mit der gleichnamigen Funktion im Betriebssystem gleichzusetzen: Es funktioniert lediglich innerhalb einer einzigen Silverlight-Anwendung.

Leider erfordert die Drag-&-Drop-Implementierung in Silverlight 2 etwas Handarbeit. Der Entwickler muss selber dafür sorgen, dass die Funktion das ausgewählte Element

– beim Drücken der linken Maustaste mit der Bewegung des Mauszeigers verknüpft,
– dass sie es beim Bewegen der Maus relativ zur Mausposition mitbewegt,
– und dass das Element beim Loslassen der linken Maustaste an seiner neuen Position bleibt und von der Maus wieder „abgekoppelt“ wird.

Im Beispiel soll der Thumbnail von einem UI-Control (*imageOverview*) in ein anderes (*thumbnailContainer*) gezogen werden (Listing 5). Dazu muss er beim Drücken der Maustaste aus seinem Parent-Control entfernt und einem Canvas hinzugefügt werden, das in der obersten Ebene der Anwendung liegt (*dragLayer*). Solange die Maustaste gedrückt bleibt, positioniert die Anwendung den Thumbnail anhand der Mausposition innerhalb des Canvas neu. Beim Loslassen der Maustaste überprüft sie, ob sich der Cursor über dem Ziel-Control (der Bilderleiste) befindet: Ist das der Fall, entfernt sie den Thumbnail aus dem *dragLayer* und fügt ihn in den *thumbnailContainer* ein – andernfalls kehrt er wieder in die Übersichtstabelle (*imageOverview*) zurück (Listing 6).

Slideshow über Timer steuern

Dabei gilt es zu beachten, dass der Hintergrund des *ScrollViewer*-Control als *background="Transparent"* definiert wird, sonst erkennt das Programm die leere Bilderleiste beim *hitTest* nicht.

Für die Slideshow benötigt die Klasse *Page.xaml.cs* drei weitere Properties: ein Flag, das besagt, ob sich die Anwendung im Slideshow-Modus befindet oder nicht (*isSlideshow*), einen Zähler, der angibt, welches Bild aus der Liste gerade zu sehen ist (*imageIndex*), sowie einen Timer, mit dessen Hilfe nach einer bestimmten Zeit eine Umschaltung zum nächsten Bild erfolgt (*slideshowTimer*) (Listing 7).

Der *slideshowButton* dient sowohl zum Starten als auch zum Anhalten der Slideshow: Je nachdem, in welchem Zustand sich die Anwendung gerade befindet, ruft sie entweder *startSlideShow* oder *stopSlideShow* auf.

Die Methode *startSlideShow* setzt das Flag *isSlideshow* und stellt die Zählervariable *imageIndex* auf *0* zurück. Anschließend erfolgt die Initialisierung der Benutzeroberfläche: Die Beschriftung des Button ändert sich, die Übersicht *imageOverview* sowie die Bilderleiste werden unsichtbar. Im Gegenzug erscheint das Image-Control (*slideshowImage*), ist aber noch transparent geschaltet. Das erste Bild wird nun zugewiesen und per Animation eingeblendet, anschließend startet der Timer, der die weitere zeitliche Steuerung der Slideshow übernimmt.

Nach Ablauf des Timers (*Eventhandler slideshowTimer _Tick*) startet die Animation zum Ausblenden des *Image*-Control. Am Ende (*fadeOutAnimation_Completed*) wird das *Source*-Attribut des *Image*-Control geändert und die Animation zum Einblenden gestartet (*showNextSlide*), danach beginnt der Prozess von vorne.

Das manuelle Beenden der Slideshow stoppt den Timer und setzt das Flag *isSlideshow* auf *false* zurück. Das *Image*-Control wird unsichtbar geschaltet und die Übersichtstabelle sowie die Bilderleiste mit den ausgewählten Bildern sind wieder zu sehen – nun kann man die Bildauswahl verändern oder neue Bilder suchen.

Für den Fall, dass man ein Flickr-Konto hat, gestaltet sich der Zugriff auf die eigenen Fotos und weitere Methoden der API nicht wesentlich anders. Viele Funktionen erfordern jedoch zuvor eine Authentifizierung, deren Umsetzung einige Zusatzschritte verlangt – die Schnittstellen-Dokumentation von Flickr liefert hier zusätzliche Hilfe.

Zu den Anforderungen an eine „reiche“ Internet-Plattform gehört heute die Fähigkeit, Videos in ansprechender Form auszuliefern. Kein Wunder also, dass Microsoft Silverlight mit erheblichen Talenten in diesem Bereich ausgestattet hat. Im

Listing 5: Verarbeiten des XML

```
void flickrService_DownloadStringCompleted(object sender,
                                          DownloadStringCompletedEventArgs e)
{
    XDocument xmlImages = XDocument.Parse(e.Result);
    if (e.Error != null ||
        xmlImages.Element("rsp").Attribute("stat").Value == "fail")
    {
        searchInput.Text = "Fehler! (" + e.Result + ")";
        return;
    }
    else
    {
        searchInput.Text = searchText;
        stopSlideShow();
        imageOverview.Children.Clear();
        thumbnailContainer.Children.Clear();
        images = from photo in
               xmlImages.Element("rsp").Element("photos").Descendants().ToList()
                 select new FlickrImage
                 {
                     Id = (string)photo.Attribute("id"),
                     Secret = (string)photo.Attribute("secret"),
                     Server = (string)photo.Attribute("server"),
                     Farm = (string)photo.Attribute("farm"),
                 };
        initializeThumbnails();
    }
}
```

Listing 6: Methoden für Drag & Drop

```
void thumbnail_MouseLeftButtonDown(object sender, MouseEventArgs e)
{
    FrameworkElement fe = sender as FrameworkElement;
    Thumbnail thumb = sender as Thumbnail;
    Point clickPosition;
    if (fe != null)
    {
        isDragging = true;
        mousePosition = e.GetPosition(null);
        clickPosition = e.GetPosition(thumb.thumbnailImage as UIElement);
        fe.CaptureMouse();
        fe.Cursor = Cursors.Hand;
        (fe.Parent as Panel).Children.Remove(fe);
        dragLayer.Children.Add(fe);
        fe.SetValue(Canvas.LeftProperty, mousePosition.X - clickPosition.X);
        fe.SetValue(Canvas.TopProperty, mousePosition.Y - clickPosition.Y);
    }
}
void thumbnail_MouseLeftButtonUp(object sender, MouseEventArgs e)
{
    FrameworkElement fe = sender as FrameworkElement;
    List<UIElement> hitElements = (List<UIElement>)HitTest(e.GetPosition(null));
    UIElement scroller = this.scroller as UIElement;
    fe.ReleaseMouseCapture();
    fe.Cursor = null;
    isDragging = false;
    dragLayer.Children.Remove(fe);
    if (hitElements.Contains(scroller))
    {
        thumbnailContainer.Children.Add(fe);
    }
    else
    {
        imageOverview.Children.Add(fe);
    }
    if (thumbnailContainer.Children.Count > 0)
    {
        this.selectionLabel.Visibility = Visibility.Collapsed;
        this.slideshowButton.Visibility = Visibility.Visible;
    }
    else
    {
        this.selectionLabel.Visibility = Visibility.Visible;
        this.slideshowButton.Visibility = Visibility.Collapsed;
    }
    mousePosition.X = mousePosition.Y = 0;
}
void thumbnail_MouseMove(object sender, MouseEventArgs e)
{
    FrameworkElement fe = sender as FrameworkElement;
    Point currentPosition = e.GetPosition(null);
    if (isDragging)
    {
        double deltaV = currentPosition.Y - mousePosition.Y;
        double deltaH = currentPosition.X - mousePosition.X;
        double newTop = deltaV + (double)fe.GetValue(Canvas.TopProperty);
        double newLeft = deltaH + (double)fe.GetValue(Canvas.LeftProperty);
        fe.SetValue(Canvas.TopProperty, newTop);
        fe.SetValue(Canvas.LeftProperty, newLeft);
        mousePosition = currentPosition;
    }
}
```


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Ein kleiner, mit Standard-Controls implementierter Videoplayer gibt Filme in Microsofts WMV-Format in guter Qualität wieder (Abb. 2).

Mittelpunkt stehen dabei vor allem eine einfache Produktion und Einbindung sowie die zunehmend höhere Bildqualität. Diverse Partnerschaften haben bereits eindrucksvolle Beispielanwendungen hervorgebracht (zuletzt die Online-Olympia-Berichterstattung in den USA von NBC) – dass dies auch im Eigenbau leicht möglich ist, soll der letzte Abschnitt des Tutorials zeigen.

Die Einbindung von Video erfolgt denkbar einfach über ein *MediaElement*-Control (Listing 8). Als Format akzeptiert Silverlight 2 zwar ausschließlich das Microsoft-eigene Windows Media Video (WMV), dieses bietet aber von Bandbreiten für mobile Clients über Streaming bis zu HD-Qualität (in Form des VC-1-Codecs, der unter anderem auf Blu-ray Discs Verwendung findet) alles, was das Produzentenherz begehrt.

Ein paar Standard-Controls zur Ansteuerung lassen schnell einen Minimal-Videoplayer entstehen (Listing 9). Wählt man eine geeignete Datei zur Wiedergabe aus (etwa einen Download in 720p-Auflösung aus Microsofts WMV HD Showcase), zeigt sich, dass „matschige“ Onlinevideos in Thumbnail-Größe mit Silverlight der Vergangenheit angehören sollten – die benötigte Bandbreite und Prozessorleistung beim Client vorausgesetzt (Abbildung 2).

Eigene Silverlight-konforme Bewegtbilder (Abbildung 3) generiert man am besten mit dem Expression Encoder 2 (dem Enkel des Windows Media Encoder, Abbildung 4), der mittlerweile Teil der Expression Suite ist und nach Ablauf einer 30-tägigen Probezeit immer noch kostenlos als abgespeckte „Express“ Edition lauffähig ist.

Das Produkt ist entweder eine WMV-Datei zur Integration in eine Anwendung oder eine schlüsselfertige Silverlight-1.0-Applikation auf Basis mehrerer zur Auswahl stehender Player-Designs (die sich sogar über Blend noch bearbeiten lassen). 2.0-Vorlagen sind noch nicht offiziell enthalten, die Ergänzung eigener Entwürfe ist allerdings möglich (siehe Tim Heuers Blog in den „Onlinequellen“).

Flickr API Keys

Um auf die Flickr-API zugreifen zu können, braucht man einen Application Key, der den Onlinedienst in die Lage versetzt, die Verwendung seiner Programmierschnittstelle zu kontrollieren. Ein kommerzieller Einsatz muss vorab genehmigt werden, allerdings kann man einen Key für die private Nutzung kostenlos anfordern: www.flickr.com/services/api/misc.api_keys.html.

Silverlight Streaming ohne Kosten

Die Kosten des Hostings von RIAs (insbesondere mit HD-Videoinhalten, die schnell einige Gigabyte belegen) können aufgrund des hohen Daten- und Transfervolumens leicht zu einem signifikanten Faktor werden.

Um seine neue Technik zu fördern und Entwicklern diesen Kopfschmerz zu nehmen, hat Microsoft bereits frühzeitig einen ergänzenden Service namens Silverlight Streaming (SLS) ins Leben gerufen (Abbildung 5 und Listing 10). Er ersetzt allerdings nicht das Hosting kompletter Websites, sondern nur das der Silverlight-Applikation oder der zugehörigen Medien-Assets.

Das kostenlose Angebot umfasst zurzeit 10 GByte Speicherplatz und 5 TByte Transfervolumen mit der Einschränkung, dass jedes Video kleiner als 105 MByte sein muss (das entspricht einem Maximum von 10 Minuten bei

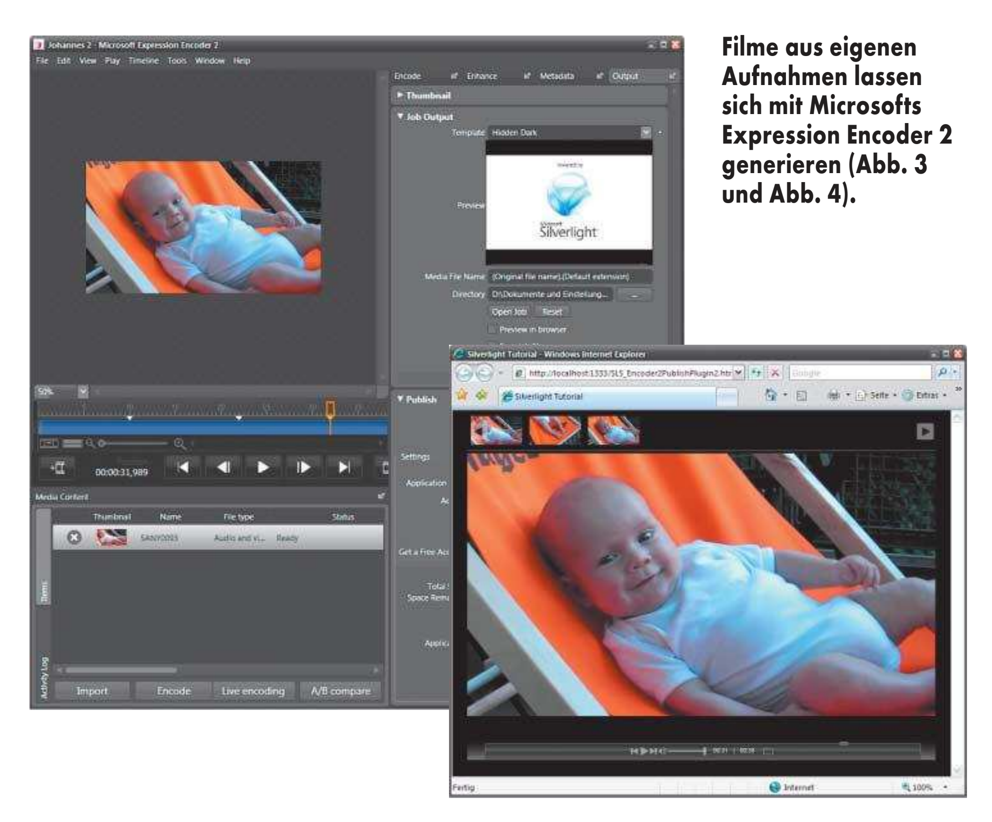
Listing 7: Methoden zum Abspielen der Slideshow

```
...
// Variablen für die Flickr-Anbindung
IEnumerable<FlickrImage> images;
private string searchText;
// Variablen für Drag & Drop
private Point mousePosition;
private bool isDragging = false;
// Variablen für die Slideshow
int imageIndex = 0;
private bool isSlideshow = false;
private DispatcherTimer slideshowTimer = new DispatcherTimer();
public Page()
{
    InitializeComponent();
    imageOverview.Visibility = Visibility.Visible;
    fadeOutAnimation.Completed += new EventHandler(fadeOutAnimation_Completed);
    slideshowTimer.Interval = new TimeSpan(0, 0, 0, 0, 5000);
    slideshowTimer.Tick += new EventHandler(slideshowTimer_Tick);
}
private void startSlideShow()
{
    isSlideshow = true;
    imageIndex = 0;
    imageOverview.Visibility = Visibility.Collapsed;
    scroller.Visibility = Visibility.Collapsed;
    slideshowImage.Opacity = 0;
    slideshowImage.Visibility = Visibility.Visible;
    slideshowButton.Content = "Slideshow anhalten";
    showNextSlide();
    slideshowTimer.Start();
}
private void stopSlideShow()
{
    slideshowTimer.Stop();
    isSlideshow = false;
    slideshowImage.Visibility = Visibility.Collapsed;
    imageOverview.Visibility = Visibility.Visible;
    scroller.Visibility = Visibility.Visible;
    slideshowButton.Content = "Slideshow starten";
}
private void showNextSlide()
{
    UIElementCollection slideshowImages = thumbnailContainer.Children;
    Thumbnail currentThumbnail;
    if (slideshowImages == null) return;
    if (imageIndex >= slideshowImages.Count) imageIndex = 0;
    currentThumbnail = (Thumbnail) slideshowImages.Skip(imageIndex).First();
    setImageSource(currentThumbnail.ImageSource, slideshowImage);
    fadeInAnimation.Begin();
    imageIndex++;
}
```


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Filme aus eigenen Aufnahmen lassen sich mit Microsofts Expression Encoder 2 generieren (Abb. 3 und Abb. 4).

Listing 8: *SimpleVideo.xaml*

```
...
<Grid Grid.Row="0">
     <MediaElement x:Name="videoElement"
                   Source="robotica_720.wmv" AutoPlay="True"
                   Height="720" Width="1280" />
</Grid>
<StackPanel Orientation="Horizontal" Grid.Row="1"
                   HorizontalAlignment="Center" VerticalAlignment="Center">
   <ToggleButton x:Name="playToggleButton" Content="Anhalten"
                 Width="100" Height="30"
                 FontFamily="Tahoma" FontSize="12" />
   <TextBlock x:Name="infoTextBlock" FontFamily="Tahoma"
              FontSize="12" VerticalAlignment="Center" Margin="10"/>
</StackPanel>
...
```

Listing 9: *SimpleVideo.xaml.cs*

```
...
public Page()
{
    InitializeComponent();
    playToggleButton.Checked += new RoutedEventHandler(playToggleButton_Checked);
    playToggleButton.Unchecked += new RoutedEventHandler(playToggleButton_Unchecked);

    videoElement.CurrentStateChanged += new RoutedEventHandler(videoElement_CurrentStateChanged);
}
void playToggleButton_Checked(object sender, RoutedEventArgs e)
{
    videoElement.Pause();
    playToggleButton.Content = "Abspielen";
}

void playToggleButton_Unchecked(object sender, RoutedEventArgs e)
{
    videoElement.Play();
    playToggleButton.Content = "Anhalten";
}

void videoElement_CurrentStateChanged(object sender, RoutedEventArgs e)
{
    if (videoElement.CurrentState == MediaElementState.Playing)
    {
        infoTextBlock.Text = String.Format("Aufloesung:{0}x{1} Pixel", videoElement.NaturalVideoWidth,
                                                            videoElement.NaturalVideoHeight);
    }
}
```

einer Datenrate von 1,4 Mbps) – mehr als genug für viele Anwendungsfälle.

Microsoft hat den Dienst in der Vergangenheit immer wieder erweitert, sodass nach dem Erstellen eines neuen Benutzerkontos oder dem Anmelden mit einem vorhandenen Windows Live Account mehrere Optionen auf der Admin-Seite zur Auswahl stehen.

Einerseits kann man komplette Silverlight-Anwendungen hochladen (1.0 manuell gepackt als ZIP-Archiv, 2.0 als XAPs), die man per *iframe* oder über ein Windows Live Control in eigene Webseiten einbinden kann (Listing 11). Die Erstellung einer *manifest.xml*-Datei mit einigen Metadaten über die Applikation kann mittlerweile online erfolgen.

Andererseits kann der Benutzer auch „nackte“ Videos einstellen – Dateien in einem von Silverlight nicht unterstützten Format transkodiert der Dienst automatisch online. Zur Einbindung steht wiederum *iframe* mit einem Standard-Player zur Verfügung (eignet sich beispielsweise für Blogs). Wer lieber mehr Kontrolle über Funktion und Design haben möchte, erhält aber auch direkten Zugriff auf die WMV-Datei. Für alle Varianten stehen zur Unterstützung passende Code-Snippets zur Verfügung.

Wer’s noch integrierter haben möchte, sollte sich das „Publish Plug-In“ für den erwähnten Expression Encoder herunterladen, mit dem das Hochladen auf SLS als Teil des Encoding-Prozesses automatisierbar ist. Die zugrunde liegende Webservice-API zur programmatischen Steuerung von Silverlight Streaming ist in einem SDK dokumentiert und steht Entwicklern zur Verfügung.

Nächste Schritte

Damit endet diese Einführung in die Programmierung mit Silverlight 2. Das mittlerweile recht ansehnliche Arsenal von UI Controls sprengt (zum Glück)

Tutorial

Teil I: Überblick Silverlight 2, Installation, Projektstruktur, erste Beispielanwendung inklusive Button und Event-Handler

Teil II: Verwendung von Standard-Controls, Interaktivität, Debugging, Einsatz von Expression Blend

Teil III: Anbindung externer Daten, Drag & Drop, Deployment auf Silverlight Streaming

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

den Rahmen dieses Tutorials und auch die mächtige .Net-Klassenbibliothek im Rücken von Silverlight könnte einige Seiten füllen. Wer den Einstieg in das relativ junge Programmiermodell mit XAML geschafft hat, sollte mit der Dokumentation des SDK bewaffnet gut weiterkommen. Die offizielle Silverlight-Webseite bietet sowohl Inspiration als auch Unterstützung im Community-Bereich.

Doch selbst wer zurzeit nicht plant, komplette Websites mit Silverlight zu erstellen, bekommt von dieser Technik Interessantes geboten. Egal, ob für die digitale Galerie der eigenen Home-Videos oder zum Bereitstellen von Screencasts: Als hochauflösende Alternative zu den einschlägig bekannten Video-Sharing-Plattformen hat man mit Silverlight, Expression Encoder 2 und Silverlight Streaming ein leistungsfähiges Gespann an der Hand. (Die Moonlight-Implementierung für Linux unterstützt zurzeit allerdings noch keine Multimedia-Funktionen.)

Zusätzlich zu den Listings auf dem *iX*-FTP-Server stehen die Beispiele zu Silverlight Streaming unter www.heldensocke.de/ix/ zur Ansicht bereit. (ka)

REGINA DOWLING

arbeitet als Multimedia-Programmiererin bei Berger Baader Hermes in München.

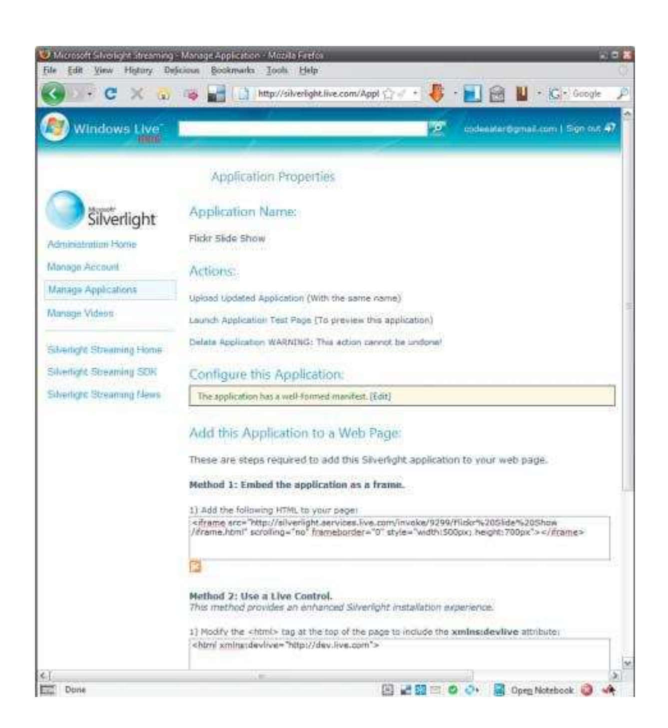
JÖRG MÜLLER

arbeitet als Head of Technology bei der Business Live GmbH in München.

iX-Link ix0810147

Firefox 3 und Silverlight

Aufgrund eines Fehlers im ursprünglichen Erkennungsskript *silverlight.js* stellt Firefox 3 Silverlight-1.0-Anwendungen nicht ohne Weiteres dar. Abhilfe schafft das Austauschen der Datei gegen die neueste Version, die im Silverlight 2.0 Beta 2 SDK enthalten ist oder separat heruntergeladen werden kann (code.msdn.microsoft.com/silverlightjs). Die Player-Vorlagen im Encoder 2 enthalten ebenfalls noch die fehlerhafte Version, können aber leicht im Templates-Ordner der Installation (beispielsweise *C:\Programme\Microsoft Expression\Encoder 2\Templates*) aktualisiert werden.



Über Microsofts Silverlight Streaming Service (SLS) können Anwender kostenlos eigene Videos im Web veröffentlichen (Abb. 5).

Listing 10: Einbindung der *FlickrSlideShow* über SLS

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xmlns:devlive="http://dev.live.com">
<head>
   <title>Silverlight Tutorial</title>
   <script type="text/javascript"
           src="https://controls.services.live.com/scripts/base/v0.3/live.js">
   </script>
   <script type="text/javascript"
           src="https://controls.services.live.com/scripts/base/v0.3/controls.js">
   </script>
</head>
<body style="background: black; margin: 0; padding: 0; font-family: Trebuchet MS, Arial; color: White;">
   <devlive:slscontrol silverlightVersion="2.0"  src="/9299/Flickr Slide Show/">
   </devlive:slscontrol>
</body>
</html>
```

Listing 11: *SimpleVideo.xaml* mit SLS Video

```
...
<MediaElement x:Name="videoElement" Source="http://silverlight.services.live.com/9299/Robotica%20720p/video.wmv"
               AutoPlay="True" Height="720" Width="1280" />
...
```

Onlinequellen

Flickr-API	www.flickr.com/services/api/flickr.photos.search.html
Drag & Drop in Silverlight 2	msdn.microsoft.com/en-us/library/cc189072(VS.95).aspx
Flickr.Net	www.codeplex.com/Wiki/View.aspx?ProjectName=FlickrNet
WMV HD Showcase	www.microsoft.com/windows/windowsmedia/musicandvideo/hdvideo/contentshowcase.aspx
Expression Encoder 2	www.microsoft.com/expression/products/overview.aspx?key=encoder
Silverlight Streaming Admin Website	silverlight.live.com
Silverlight Streaming Blog	dev.live.com/blogs/sls/
Silverlight Streaming SDK	msdn.microsoft.com/en-us/library/bb851621.aspx
Silverlight 2 Video Player als Encoder-2-Vorlage	timheuer.com/blog/archive/2008/07/16/silverlight-2-video-player-encoder-template.aspx
Silverlight Streaming Publishing Plug-In für Expression Encoder 2	www.microsoft.com/downloads/details.aspx?FamilyID=0708e7d79ba1-448e-9c82-3d71e8979a1b&displaylang=en

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Geodatendienste mit dem UMN-Mapserver effizient verwalten

Kartenmacher

Jens Schumacher

Der Mapserver der Universität von Minnesota eignet sich nicht nur zum Bereitstellen eigener Daten, sondern auch zur Verwaltung von Geodatendiensten. Dabei erweist sich die Programmierschnittstelle Mapscript-API als große Hilfe.

Standardisierte Geodatendienste anzubieten ist für viele Unternehmen und öffentliche Einrichtungen zunehmend wichtiger, da diese die Kernkomponenten in wachsenden und flexiblen Geodateninfrastrukturen bilden. Der Mapserver der Universität von Minnesota (UMN) [1] bietet durch seine Mapscript-API einen effizienten Weg, Geodatendienste zu veröffentlichen.

Beim Austausch von Geodaten kommen verstärkt standardisierte Dienste zum Einsatz. Das resultierende Netz aus Datenanbietern und -konsumenten im Verbund mit der eingesetzten Technik bezeichnet man als Geodateninfrastruktur. Solche Infrastrukturen haben sich vor allem in der öffentlichen Verwaltung auf verschiedenen räumlichen und hierarchischen Ebenen etabliert, etwa das europäische INSPIRE oder die deutschlandweite GDI-DE.

Dienstbasierte Infrastrukturen bieten eine Reihe von Vorteilen:
– Sie vermeiden Datenredundanz.
– Die Verwaltung der Geodaten bleibt in den Fachbereichen.
– Daten haben eine höhere Aktualität und einen einheitlichen Stand.
– Software kann auf Basis der Standards entwickelt werden; Softwarekomponenten einer GDI lassen sich leichter austauschen.
– Datenkonsumenten können Geodaten beliebig kombinieren und überlagern.

Das Open Geospatial Consortium (OGC), eine internationale Organisation aus Vertretern von Industrie, Forschungs- und Regierungsorganisationen, hat eine Reihe von Diensten spezifiziert. Zu den vom UMN-Mapserver unterstützten zählen der Web Map Service (WMS), der Web Feature Service (WFS) und der Web Coverage Service (WCS).

In der Regel gibt der Web Map Service Kartenansichten in Form von Grafiken zurück. Zusätzlich lassen sich Sachdaten zu einem Kartenpunkt abrufen. Im Gegensatz dazu liefert ein Web Feature Service Vektordaten, die im XML-Dialekt Geography Markup Language (GML) kodiert sind. WFS-Clients bieten in der Regel mehr Funktionen und eine „lebendigere“ Darstellung als WMS-Clients. Der Web Coverage Service erlaubt den Zugriff auf Rohdaten – vor allem Rasterdaten –, die sich im Client analysieren, modellieren und darstellen lassen.

Dienstzugriff per Mapfile

Grundlage jeglicher Konfiguration mit dem UMN-Mapserver ist das Mapfile. Geodatendienste lassen sich über das Common Gateway Interface Programm des UMN-Mapservers abfragen; die URL www.fqnserver.de/cgi-bin/mapserv?map=/map/grundlagen.map&service=WMS&request=getCapabilities&version=1.1.1 etwa ruft Daten eines WMS ab. Der Parameter *map* teilt dem CGI-Programm das gewünschte Mapfile mit. Die übrigen Argumente sind vom OGC für den jeweiligen Dienst spezifiziert; *service* gibt den gewünschten Dienst an, in diesem Fall *WMS*.

Es ist möglich, über ein Mapfile mehrere Geodatendienste anzubieten. Listing 1 zeigt die Konfiguration eines WMS und eines WFS in einem Mapfile. Die meisten der für Geodatendienste relevanten Einträge haben ein Präfix, das den Dienst identifiziert, etwa *wfs_* oder *wms_*. Die Werte von Konfigurationsparametern wie *wfs_title* und *wms_title* können sich wiederholen. In neueren Versionen des UMN-Mapservers lässt sich mit dem Präfix *ows_* ein Parameter für beide Dienste setzen: *ows_title* gibt den Titel sowohl für WMS als auch für WFS an.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Allerdings besitzt die Zugriffsmethode über CGI zwei Nachteile: Erstens lassen sich Anfragen und Antworten nicht mit eigener Programmlogik modifizieren. Zweitens sind die Inhalte der Mapfiles hochgradig redundant. Das macht sich vor allem in komplexeren Geodateninfrastrukturen unangenehm bemerkbar.

Redundanz erhöht den Konfigurations- und Wartungsaufwand. Wechselt etwa ein Server den Namen, muss der Administrator in allen betroffenen Mapfiles die Parameter *wms_online resource* und *wfs_onlineresource* ändern. Auch die Kontaktangaben, etwa *wms_address* oder *wms_contactper son*, muss man bei Veränderungen händisch anpassen. Metadaten zu Geodaten werden oft als eigene zentrale Dienste angeboten. Das führt dazu, dass sie doppelt vorkommen: einmal im Mapfile und einmal als spezialisierter Metadatendienst. Obendrein wächst bei der CGI-Methode der Verwaltungsaufwand mit der Zahl der HTML-Templates, die man zum Beispiel für *getFeatureInfo*-Anfragen benötigt.

Bestimmte Geodatendienste sollen nur authentifizierten Nutzern zur Verfügung stehen, oft in unterschiedlichen, von der Nutzerkennung abhängigen Ansichten. Verwendet man das CGI-Interface, lässt sich ein anmeldungspflichtiger Geodatendienst jedoch nur mit einem zusätzlichen Authentifizierungsserver verwirklichen.

Hinzu kommt die Frage der Autorisierung, die eng mit dem angebotenen Dienst verknüpft ist. Ein räumlich oder inhaltlich eingeschränkter Zugriff zum Beispiel – auf Karten eines begrenzten Gebiets oder auf bestimmte Objekte –, ist ohne Eingriffe in die Logik des Geodatendienstes nur schwer zu realisieren. Dasselbe gilt für ein gezieltes Logging der Zugriffe.

Vereinfachen und erweitern

Seit Version 4.9 des UMN-Mapservers kann man mit der Mapscript-API in den Ablauf einer Serviceanfrage eingreifen. Dadurch lässt sich die Verwaltung von Geodatendiensten erheblich

Listing 1: Konfiguration eines WMS und WFS in einem Mapfile

```
MAP
  ...
  WEB
    IMAGEPATH "/data/web/tmp/"
    IMAGEURL "/tmp/"
    METADATA
      "wms_title"              "Grundlagenkarte"
      "wms_srs"                "epsg:31467 epsg:4326 epsg:25832"
      "wms_onlineresource"
"http://www.fqnserver.de/cgi-bin/mapserv?map=/map/grundlagen.map&"
      "wms_stateorprovince"    "BY"
      ...
      "wfs_title"              "Grundlagenkarte"
      "wfs_srs"                "epsg:31467 epsg:4326 epsg:25832"
      "wfs_onlineresource"
"http://www.fqnserver.de/cgi-bin/mapserv?map=/map/grundlagen.map&"
      "wfs_stateorprovince"    "BY"
      "ows_schemas_location"
"http://schemas.opengeospatial.net/"
      ...
  END

  LAYER
    NAME "gewaesser"
      TYPE "polygon"
      DUMP TRUE
      METADATA
        "wms_title"            "Gewässer"
        "wms_srs"              "epsg:31467 epsg:4326 epsg:25832"
        ...
        "wfs_title"            "Gewässer"
        "wfs_srs"              "epsg:31467 epsg:4326 epsg:25832"
        "gml_featureid"        "ID"
        "gml_include_items"    "all"
  END
  ...
END
```



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 2: OGC Web Service Dispatcher

```
<?php
...
$oMap = ms_newMapObj("/map/grundlagen.map");
$oMap->moveLayerUp(2);
ms_ioinstallstdouttobuffer();
$oMap->owsdispatch($request);
$contenttype = ms_iostripstdoutbuffercontenttype();
header('Content-type: '.$contenttype);
ms_iogetStdoutBufferBytes();
ms_ioresethandlers();
?>
```

Listing 3: Zentrale Steuerung der Dienste

```
<?php
...
if (!extension_loaded("MapScript")) {
   dl("php_mapscript.so");
}
$themen["grundlagenkarte"]="/map/grundlagen.map";
$themen["fachdatenkarte"]="/map/fachdatenkarte.map";

$oMap = ms_newMapObj($themen[$_REQUEST["service_name"]]);

if (strtoupper($_REQUEST["request"]) ==
"GETCAPABILITIES" &&
    strtoupper($_REQUEST["service"]) == "WMS") {

   $online_resource="http://".SERVER."/ows.phtml?
service_name=".$_REQUEST["service_name"]."&";
   $oMap->setmetadata("wms_onlineresource",
      $online_resource);

   $oMap->setmetadata("wms_abstract", insertWSMetadata
      ("http://meta.geospatialdata.de?id=34", "WMS"));

   $map->setmetadata("wms_stateorprovince",
      iconv("ISO-8859-1", "UTF-8", "Thüringen"));
}
$oMap->owsdispatch($request);
...
?>
```

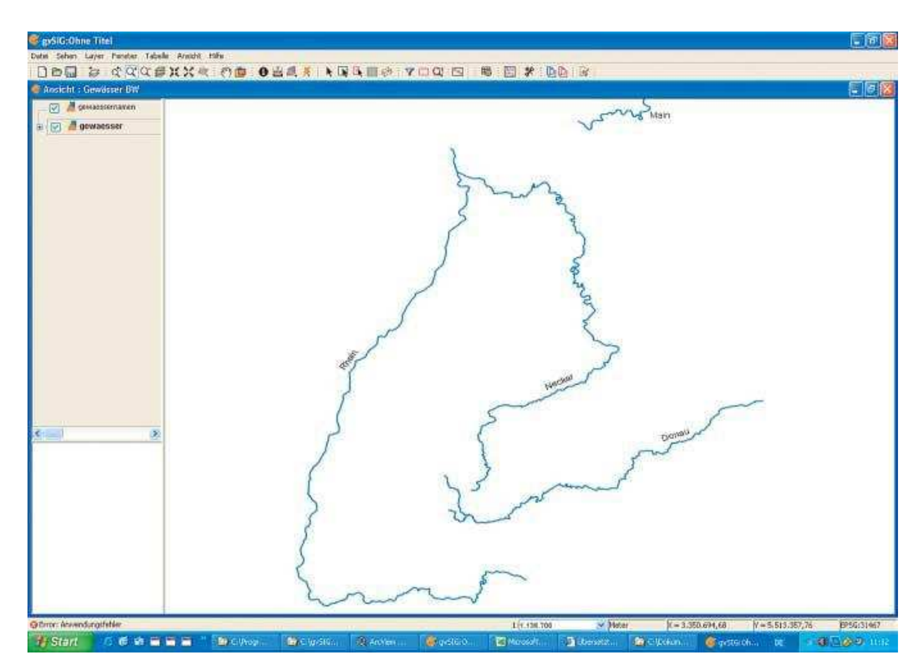
Listing 4: Abfrage von Punktinformationen

```
<?php
...
$oMap = ms_newMapObj($themen[$_REQUEST["service_name"]]);
if (strtoupper($_REQUEST["request"]) == "GETFEATUREINFO" &&
    strtoupper($_REQUEST["service"]) == "WMS") {
   echo displayWMSFeatureInfoAsHTML($oMap,$_REQUEST);
   exit(0);
}
?>
```

Listing 5: Filterung der Kartenansicht

```
<?php
...
$oMap = ms_newMapObj($themen[$_REQUEST["service_name"]]);
$gewaesser = $oMap->getLayerByName("gewaesser");
if ($user.has_role("art_1024")) {
   $gewaesser->setFilter(" art = '1024'");
}
$oMap->owsdispatch($request);
...
?>
```

vereinfachen. Listing 2 zeigt, wie der Mechanismus funktioniert. Der Konstruktor *ms_newMapObj()* erzeugt ein neues Map-Objekt, das mit dem angegebenen Mapfile verknüpft ist. Mit den Funktionen der Mapscript-API lassen sich die im Mapfile konfigurierten Parameter ergänzen oder ändern; *moveLayerUp()* etwa ändert die Reihenfolge der Layer. Das modifizierte Map-Objekt dient anschließend als Grundlage für die Antwort des Geodatendienstes. *owsdispatch()* schließlich stellt das Resultat im gewünschten Format bereit.



Röntgenblick: Mit Filtern lässt sich die Kartenansicht auf bestimmte Objekte beschränken (Abb. 1).

Dadurch lässt sich ein zentrales Steuerungsskript für alle Geodatendienste entwickeln, das die genannten Nachteile vermeidet. Listing 3 zeigt schematisch den Programmablauf bei einer *getCapabilities*-Anfrage für einen Web Map Service. An zentraler Stelle setzt das Skript die URL für die *wms_onlineresource* für alle WMS-Dienste des Anbieters. Clients nutzen sie, um den Web Map Service einzubinden. Die XML-kodierte Antwort gibt Aufschlüsse über die Ressourcen des Dienstes: Kartenlayer, Abfragemöglichkeiten, räumliche Abdeckung, unterstützte Bildformate sowie Kontaktdaten des Dienstanbieters.

Informationen zu einem Punkt der Karte lassen sich mit der Mapscript-API ins HTML-Format wandeln. Es ist daher nicht mehr nötig, für den *getFeatureInfo*-Request den Template-Mechanismus des Mapservers zu bemühen (Listing 4).

Wie man den Anzeigeumfang für einen bestimmten Nutzer modifizieren kann, demonstriert Listing 5. Der Filter beschränkt die Ansicht auf bestimmte Objekte, in diesem Fall Gewässer, deren Attribut *art* den Wert *1024* hat.

Zwar beziehen sich alle Beispiele auf einen Web Map Service. Sie lassen sich jedoch in ähnlicher Form auf die anderen vom Mapserver unterstützten Geodatendienste anwenden.

Fazit

Mit der Mapscript-API des UMN-Mapservers lassen sich die Nachteile vermeiden, die bei einer dateibasierten Konfiguration von Geodatendiensten auftreten. Teile der Konfiguration, die sich bei mehreren Diensten wiederholen – etwa Kontaktdaten oder Servernamen – kann der Administrator zentral verwalten, zum Beispiel in einer Datenbank. Dienstspezifische Angaben wie die Visualisierungsanweisungen lassen sich im Mapfile konfigurieren. Außerdem kann man Geodatendienste mit zusätzlichen Funktionen anreichern und domainspezifische Lösungen für Autorisierung und Logging eng an die Logik des Geodatendienstes koppeln. (mr)

JENS SCHUMACHER

plant die OGC Web Service Infrastruktur mit Open-Source-Software für das Landesamt für Geologie, Bergbau und Rohstoffe im Regierungspräsidium Freiburg.

Literatur

[1] Christian Wilk; Open-Source-GIS; Auf dem Präsentierteller; Geodaten mit dem UMN-Mapserver anbieten; *iX* 9/2006, S. 136





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Netz-Traffic aufzeichnen und abspielen

Aus der Konserve

Michael Riepe



Netzadministratoren können ihre Augen nicht überall haben. Vorgänge im Netz lassen sich jedoch leicht protokollieren – und mit *tcpreplay* bei Bedarf sogar wiederholen.

Das Netz ist ein Dschungel, in dem allerlei unfreundliches Getier lauert. Zwar halten Zäune und Stacheldraht viele Angriffe ab. Sie sind jedoch nicht unüberwindlich. Außerdem ist völliges Abschotten nur selten praktikabel.

Wer etwa Dienste öffentlich anbietet, muss eine Tür für die Besucher offen lassen – und sie gut bewachen. Nicht allein, damit er auf gezielte Angriffe und Vandalismus schnell reagieren kann: Wer effektive Gegenmaßnahmen installieren will, muss die Taktik des Angreifers studieren, am besten anhand einer Aufzeichnung. Sie lässt sich später außerdem als Prüfwerkzeug für die verbesserten Sicherheitsvorkehrungen verwenden.

Kameras und Mikrofone

Aufzeichnungen lassen sich zum Beispiel mit *tcpdump* herstellen. Übergibt man dem Programm beim Start die Option *–w <dateiname>*, schreibt es die empfangenen Pakete in die angegebene Datei. Deren Inhalt lässt sich anschließend mit *tcpdump –r <dateiname>* auf der Konsole ausgeben.

Allerdings speichert *tcpdump* normalerweise nur den Anfang jedes Pakets – gewöhnlich die ersten 68 oder 96 Byte. Für die Analyse von Angriffen, die zum Beispiel auf Pufferüberläufen basieren, benötigt man jedoch in der Regel auch die übertragenen Nutzdaten. Es empfiehlt sich daher, mit der Option *–s 65535* die Menge der zu speichernden Daten auf den Maximalwert zu setzen.

Wer eine Daueraufzeichnung anfertigen will, sollte bedenken, dass Plattenplatz nicht unendlich ist. *tcpdump* trägt dem mit der Option *–C <mb>* Rechnung: Hat die Aufzeichnungsdatei die angegebene Größe (in Millionen Byte) erreicht, legt das Programm eine neue an. Nicht mehr benötigte Dateien kann man löschen. Allerdings überschreibt *tcpdump* nach einem Neustart vorhandene Dateien gleichen Namens. Wer das vermeiden will, sollte Datum und Uhrzeit als Teil des Namens verwenden, etwa mit *tcpdump –w tcpdump-`date +%Y%m%d-%H%M%S`.log*.

Für Momentaufnahmen eignet sich das Programm *pcapture*. Es liest alle Pakete mit, gibt sie jedoch nicht aus. Bricht man es mit einem der Signale *HUP*, *INT* oder *TERM* ab – etwa durch Drücken der Tastenkombination *Strg+C* –, speichert es die letzten 500 in die mit *–w* angegebene Datei. Mit der Option *–c <pakete>* lässt sich ein größerer oder kleinerer Wert einstellen. Wie bei *tcpdump* kann man mit *–i <name>* eine Netzschnittstelle wählen oder einen Filterausdruck als Argument übergeben.

Wer mit der Kommandozeile auf dem Kriegsfuß steht, kann zum Aufnehmen auch *wireshark* (vormals *ethereal*) verwenden [1]. Allerdings eignen sich die textbasierten Werkzeuge besser zum Überwachen entfernter Rechner als der grafische „Kabelhai“.

Onlinequellen

tcpdump	www.tcpdump.org
pcapture	linux.maruhn.com/sec/pcapture.html
wireshark	www.wireshark.org
tcpslice	ftp://ftp.ee.lbl.gov/tcpslice.tar.gz
tcpreplay	tcpreplay.synfin.net/trac/

Schneiden und Kopieren

Mit *tcpdump*, *pcapture* oder *wireshark* erzeugte Dateien lassen sich mit *tcpslice* nachbearbeiten. *tcpslice <datei1> <datei2>* hängt die Eingabedateien hintereinander und schreibt das Ergebnis auf die Standardausgabe oder in eine mit *–w <datei>* angegebene Datei. Ruft man *tcpslice <von> <bis> <datei>* auf, kopiert es ausschließlich Pakete, deren Zeitstempel zwischen den angegebenen Werten liegen. Zeitangaben dürfen absolut – in Sekunden seit dem 1.1.1970 – oder relativ zum Dateianfang beziehungsweise zur Startzeit sein: *tcpslice +0 +60 <datei>* etwa kopiert die erste Minute der angegebenen Datei.

Aufzeichnungen lassen sich mit *tcpreplay* wieder ins Netz einspeisen – in der Voreinstellung unverändert und mit derselben Geschwindigkeit wie bei der Aufnahme. Falls nötig, lassen sich jedoch eine Reihe von Parametern ändern, darunter die MAC- und IP-Adressen sowie die TCP- und UDP-Portnummern von Sender und Empfänger. Dabei korrigiert *tcpreplay* auch die Prüfsummen der IP-Pakete. Wer eine Datei nur bearbeiten, aber nicht senden will, kann dafür das Programm *tcprewrite* verwenden, das mit zum Paket gehört.

Das Sendetempo lässt sich mit *–x <faktor>* oder gegenüber der Aufnahme um einen bestimmten Faktor erhöhen oder senken. Man kann jedoch auch mit *–p <pakete>* oder *–M <mbps>* ein bestimmtes Tempo in Paketen oder MBit pro Sekunde vorgeben. Mit der Option *–t* sendet *tcpreplay* so schnell es die Hardware zulässt. So lassen sich zum Beispiel DoS-Angriffe simulieren oder Lasttests an Routern und Switches durchführen. Die Option *–o* hingegen schaltet das Programm auf Superzeitlupe: Drückt man eine Taste, sendet *tcpreplay* ein einzelnes Paket. Ähnlich wie mit einem Debugger kann der Admin den Ablauf der Ereignisse Schritt für Schritt verfolgen. (mr)

Literatur

[1] Thomas Kaufmann; Netzwerk-Diagnose; Auf Päckchenfang; Paketanalyse mit Ethereal; *iX* 5/2005, S. 153

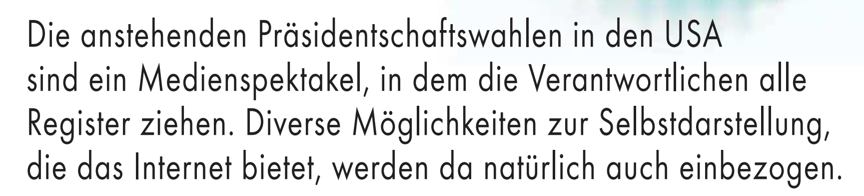




© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Präsidentschaftswahlen in den USA

Meet your president



Diane Sieger

Die anstehenden Präsidentschaftswahlen in den USA sind ein Medienspektakel, in dem die Verantwortlichen alle Register ziehen. Diverse Möglichkeiten zur Selbstdarstellung, die das Internet bietet, werden da natürlich auch einbezogen.

Kaum zu glauben, dass es schon wieder vier Jahre her ist, dass sich die Internet-Infos mit dem Präsidentschaftswahlen in den Vereinigten Staaten von Amerika befasst haben (www.heise.de/ix/artikel/2004/11/158/). Seitdem hat es viele technische Entwicklungen gegeben, von denen die diesjährigen Kandidaten ausführlich Gebrauch machen.

Leser, die ihr Wissen um das amerikanische Wahlverfahren grundsätzlich auffrischen möchten, sollten sich zunächst die Q&A-Seite der amerikanischen Botschaft in Deutschland anschauen. Unter amerikadienst.usembassy.de/us-botschaft-cgi/ad-detailad.cgi?lfdnr=2205 gibt es sämtliche wissenswerte Details rund um das Wahlsystem und wie es funktioniert. Auch die Landeszentrale für Politische Bildung Baden-Württemberg liefert gutes Hintergrundwissen unter www.lpb-bw.de/uswahl/index.php.

Wer das Geschehen aus der Ferne betrachtet, bekommt leicht den Eindruck, dass es in Amerika lediglich zwei Parteien gibt, zwischen deren Kandidaten es eine Entscheidung zu treffen gilt. Weit gefehlt. Wikipedia (de.wikipedia.org/wiki/Pr%C3%A4sidentschaftswahl_in_den_Vereinigten_Staaten_2008#Kandidaten) klärt darüber auf, dass es neben dem Demokraten Barack Obama und dem Republikaner John McCain sage und schreibe elf weitere Präsidentschaftsanwärter gibt. Bei einigen kann man sich jedoch nur kopfschüttelnd wundern, wie sie es auf diese Liste geschafft haben. Da gibt es etwa den wegen Bedrohung des derzeitigen Präsidenten George W. Bush bereits vom amerikanischen Geheimdienst vernommenen Kandidaten der „Vampire-, Hexen- und Heiden-Partei“ (www.columbiachronicle.com/paper/arts.php?id=3525). Oder Gene Amondson, den Kandidatan der Prohibition Party (www.prohibitionists.org), die schon seit 1867 für ein umfassendes Alkoholverbot kämpft. Da jedoch keiner dieser Volksvertreter auch nur den Hauch einer Chance auf die Präsidentschaft in den anstehenden Wahlen hat, soll es im Weiteren um die beiden im Rampenlicht sehenden Hauptkandidaten, Barack Hussein Obama und John Sidney McCain, gehen.

Kandidat mit eigenem Netz

Dazu zunächst ein Blick auf die Webseiten der beiden. Eine genaue Wiedergabe dessen, was man dort vorfindet, gestaltet sich ein wenig schwierig, denn da jetzt die heiße Zeit der Wahlkampfphase beginnt, nehmen die Betreiber laufend Änderungen an den Webseiten vor. War gestern bei Obama noch ein Spendenaufruf dem eigentlichen Internetauftritt vorgeschaltet, erwartet man diesen heute vergeblich. Stattdessen hat McCain sein großes Wahlversprechen auf Seite eins gepackt, das vor wenigen Tagen noch nicht dort war. Wie immer die Seite jedoch aufgebaut ist, wer erstmal im Hauptangebot von www.barackobama.com angelangt ist, bekommt alles geboten, was das Wählerherz begehrt: Pressemitteilungen, Videobotschaften, die Möglichkeit sich zur Freiwilligenarbeit zu verpflichten, Infos zum Empfang von SMS, Obama Blog und eine Übersicht, in welchen Onlinenetzwerken Obama vertreten ist (Facebook, Myspace, Youtube, Flickr, LinkedIn und so weiter und so fort). Natürlich fehlt auch der Link zum Obama Store unter store.barackobama.com nicht, der nach dem selben Muster gestrickt ist wie die Webseite: klar, übersichtlich, benutzerfreundlich.

Ein bisschen unruhiger sieht es dagegen bei John McCain (www.johnmccain.com) aus – die Webseite wirkt zunächst weniger strukturiert und es dauert einen Moment, bis man den Überblick erlangt hat. Ansonsten sind in McCains Webauftritt ähnliche Inhalte zu finden wie bei Obama, jedoch fehlt auf den ersten Blick die Selbstdarstellung in populären Onlinenetzwerken. Erst nach ein bisschen herumklicken kommt man zu McCain auf Facebook, Myspace und Youtube. Die typischen Nutzer sind vielleicht auch nicht ganz seine Zielgruppe.

Obama hingegen hat sogar sein eigenes Netzwerk gegründet: Unter my.barackobama.com gibt es in Facebook-Manier Kontaktlisten mit Freunden, Event-Übersichten, Nachrichtenversand und jeder Account kommt inklusive Blog, in dem über Obama berichtet werden kann; sehr Web-2.0-mäßig. In manchen Staaten gibt es auch Face-to-Face-Treffen der My.BarackObama.com-Community – Timothy Moenk hat ein solches Treffen besucht und berichtet unter tmoenk.typepad.com/tmoenk/2007/02/mybarackobamaco.html darüber.

Warum Obama über ein so außergewöhnlich großes Onlinenetzwerk verfügt und McCain nicht, lässt sich mithilfe eines Youtube-Videos herausfinden. Doch nicht nur über diesen Sachverhalt klärt www.youtube.com/watch?v=gz7zx2M6FWE auf. Auch der Frage, wie das Internet im Allgemeinen die Darstellung des politischen Geschehens verändert hat – insbesondere in Bezug auf die US Wahlen – geht dieses englischsprachigen Video nach.

Natürlich ist die Präsidentschaftswahl ein wichtiges Ereignis in den USA, und selbstverständlich kostet ein Wahlkampf viel Geld. Ob jedoch die Ausgabe von fünf Milliarden Dollar gerechtfertigt ist, bleibt zu bezweifeln. Immerhin hat der Wahlkampf im Jahr 2004 nur knapp eine Milliarde Dollar verschlungen, wie der Focus bereits im April unter www.focus.de/politik/schlagzeilen?day=20070420&did=381805 zu berichten wusste. Mit diesem Geld hätte man

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

sicherlich eine ganze Menge sinnvoller Arbeit finanzieren können.

Viel Aktuelles zum Thema gibt es auch bei Scot W. Stevenson – nominiert für den Grimme Online Award 2007 – zu lesen. Er ist der Meinung, dass kein Land deutsche Nachrichten und Blogs so dominiere wie die USA, will aber die Reihe der deutschsprachigen Blogs nicht mit einem weiteren ergänzen, der das Land „entweder als des Satans neue Heimat verdammt oder es als das neue Paradies vergöttert“, sondern mit einem, der die „USA erklärt“ (usaerklaert.wordpress.com). Hier bekommt man unter anderem über einen Link Einblick in Finanzunterlagen von Sarah Palin.

Bis zum Wahltag auf dem Laufenden zu bleiben stellt übrigens keine schwere Übung dar; sämtliche große Tageszeitungen berichten in ihrem Onlineangebot ununterbrochen über kleine und große Verwicklungen aus den USA. Die Süddeutsche Zeitung beispielsweise bietet unter dem Titel „Spezial US-Wahlkampf“ Neuigkeiten, sobald sich auf der anderen Seite des großen Teichs etwas Wahlspezifisches regt (www.sueddeutsche.de/politik/59/301056/uebersicht/). Beim Tagesspiegel heißt das Ganze schlicht „US Wahl“ und kann unter www.tagesspiegel.de/politik/international/us-wahl/ stets aktuell abgerufen werden. Die tagesaktuelle Präsidentschaftsvorhersage gibt es bei Pollyvote (www.pollyvote.com). Im letzten Wahljahr lag die Prognose lediglich 0,3 Prozentpunkte daneben, die veröffentlichten Daten darf man also durchaus ernst nehmen.

Wie schon zur letzten Wahl wird www.betavote.com in den nächsten Wochen der Frage nachgehen, wie die Wahlen in den USA ausgehen würden, dürfte die ganze Welt mitwählen. Einfach mal vorbeisurfen und die eigene Stimme abgeben – es wird wieder spannend zu sehen, ob es Unterschiede zwischen inner- und außeramerikanischem Wahlverhalten gibt.

Und wer es nun kaum noch erwarten kann, dem neuen amerikanischen Präsidenten zuzujubeln, für den gibt es noch einen kleinen Zeitvertreib bis zum Wahltag: Unter www.miniclip.com/games/presidential-pounding/en kann man sich einen Boxkampf mit dem Präsidentschaftskandidaten liefern, den man weniger leiden kann. (ka)

URLs auf einen Blick

www.heise.de/ix/artikel/2004/11/158/
amerikadienst.usembassy.de/us-botschaft-cgi/ad-detailad.cgi?lfdnr=2205
www.lpb-bw.de/uswahl/index.php
de.wikipedia.org/wiki/Pr%C3%A4sidentschaftswahl_in_den_Vereinigten_Staaten_2008#Kandidaten
www.columbiachronicle.com/paper/arts.php?id=3525
www.prohibitionists.org
www.barackobama.com
store.barackobama.com
www.johnmccain.com
my.barackobama.com
tmoenk.typepad.com/tmoenk/2007/02/mybarackobamaco.html
www.youtube.com/watch?v=gz7zx2M6FWE
www.focus.de/politik/schlagzeilen?day=20070420&did=381805
usaerklaert.wordpress.com
www.sueddeutsche.de/politik/59/301056/uebersicht
www.tagesspiegel.de/politik/international/us-wahl
www.pollyvote.com
www.betavote.com
www.miniclip.com/games/presidential-pounding/en

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/10/158/) hinzuzufügen.

Vor 10 Jahren: Lethargie, nein danke

Vor 10 Jahren wurde das Internet erstmals von allen Parteien zur Selbstdarstellung benutzt und stand als Plattform für aktive Wähler zur Verfügung.

Mit der Nominierung von Frank-Walter Steinmeier zum Kanzlerkandidaten der SPD hat der Bundestagswahlkampf begonnen. Wie das Duell mit Angela Merkel auch ausgeht, das Netz wird eine wichtige Rolle spielen.

Vor 10 Jahren berichtete *iX* im Artikel „Weg mit der Lethargie“ über die Internet-Aktivitäten der Parteien sowie über die sonstige netzbasierte Wahlberichterstattung. Erstmals hatten alle großen Parteien ihre Wahlprogramme online gestellt, auch wenn sie mitunter nicht einfach zu finden oder auszudrucken waren.

Bei der CDU verbarg sich das Wahlprogramm hinter einer „hutzeligen Deutschlandfahne“, die angeklickt werden musste. Ihr Internet-Auftritt galt vor 10 Jahren als der modernste, weil zum Angebot Internet-Chats mit Politikern zählten. Als älteste Partei punktete die SPD mit dem ältesten Angebot, dem virtuellen Ortsverein der SPD (VOV), ursprünglich im Onlinedienst Compuserve angesiedelt und bis heute existent.

„Der Fluff der Wahlversprechen“, den *iX* damals kritisierte, ist auch nach 10 Jahren wohlbekannt. Doch die Arbeit der Politiker zwischen den Wahlkämpfen ist etwas transparenter geworden, genau wie dies der Artikel damals wünschte. Angebote wie Abgeordnetenwatch.de, die auch von Suchmaschinen erfasst werden, führen zu einem Dialog zwischen Bürgern und Politikern. Auch wenn sich immer noch einige Politiker weigern, auf Fragen einzugehen, traut sich niemand mehr, das Internet als „Zeitverschwendung“ abzutun.

Was sich hingegen nicht geändert hat, ist offenbar die Häme gegenüber Politikern, die mit einem neuen Medium unbefangen experimentieren. Vor 10 Jahren startete für die SPD der designierte Wirtschaftsminister (und IT-Fachmann) Jost Stollmann mit einem sehr persönlichen Wahlkampftagebuch. Für dieses Experiment, das man heute als Blog bezeichnen würde, erntete Stollmann Hohn und Spott. Noch vor der Wahl gab er als Schattenminister auf.

Ähnlich erging es dieser Tage dem SPD-Generalsekretär Hubertus Heil, der versuchte, mit Twitter die Politik zu kommentieren. Dafür bekam er reichlich Spott vom „Spiegel“, dessen Autor die Technik des Microbloggens offenbar nicht verstanden hatte. Spott und vor allem Kritik kassierte damals auch die Firma Microsoft, die einen Wettbewerb für ihren „Road Ahead-Prize“ ausgeschrieben hatte: Gewinnen sollte ihn die Schulklasse mit der informativsten Webseite zum Thema Bundestagswahl 1998. Prompt gab es Vorwürfe, dass Microsoft die Schüler vom „eigentlichen“ Thema Politik abhalten würde.

Inhaltlich spielte das Internet im Wahlkampf vor 10 Jahren keine Rolle. Die Ausnahme war wiederum Jost Stollmann, der vordringlich die Initiative „Schulen ans Netz“ fördern wollte. Dieser Punkt hat sich entscheidend geändert. Dank Web 2.0 ist der gläserne Bürger ein wichtiges Wahlkampfthema geworden – Sicherheit im Netz dürften in den nächsten Monaten auch Politiker und Politikerinnen anmahnen, die nicht einmal wissen, was ein Browser ist.

Detlef Borchers

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

MEHR KBYTES

Windows-Programmierung

Innerhalb der Programmieruniversen hat das Microsoftsche All schon immer eine Sonderstellung gehabt. (Visual) Basic und C# gehören fest in sein Sternensystem, das .Net-Framework und der Webserver IIS ebenso. Selbst Verlage, die aus einer der Unix-Galaxien beziehungsweise einem Open-Source-Gürtel stammen, haben diese Parallelwelt längst entdeckt und versorgen ihre Entwickler mit Lektüre. Richtschnur bleibt mindestens gelegentlich, was die hauseigene Microsoft Press zu sagen hat.

Auf einer Seite Neuerscheinungen zur Windows-Programmierung zusammenzustellen kann nur den Charakter des Fragmentarischen haben. Hier soll es um neue Bände zu C#, .Net-Aspekte und den ISS gehen. SQL Server, Basic und Windows Server fehlen demzufolge.

Die Besprechung des Hanser-Bandes zu Visual C# 2008 auf Seite 162 behandelt nur eins der Bücher, die diese Programmiersprache zum Inhalt haben. Bei der Microsoft Press haben Dirk Louis und Shinja Strasser auf fast ebenso vielen Seiten wie Gewinnus und Doberenz die Grundlagen der C#-Programmierung ausgebreitet. Schon im Untertitel kommt allerdings der Begriff „Profi-Know-how“ vor; nicht zu Unrecht, denn allein in die objektorientierte Programmierung führen die Autoren auf circa 140 Seiten ein.

Außer den üblichen Spracheigenschaften (von Variablen über Operatoren bis zu Arrays) behandeln sie das fortgeschrittene Arbeiten mit C# sowie „nützliche“ .Net-Klassen, Windows Forms inklusive Windows Presentation Foundation (WPF) sowie Multithreading und Datenbankprogrammierung. Den Web Forms und Webservices sowie der Language Integrated Query (Linq) sind eigene Kapitel gewidmet. Sicherlich zum Selbststudium wie als Nachschlagewerk geeignet.

Wrox, bekannt durch seine knallroten dicken Paperbacks und mittlerweile bei Wiley angesiedelt, hat, was den Umfang eines C#-Buchs angeht, den Vogel abgeschossen. 1782 englischsprachige Seiten dürften selbst den lesegierigsten Programmierer fordern. Es überrascht deshalb nicht, dass die fünf Autoren einen reichlichen Strauß an Themenbereichen binden mussten, um auf diesen Umfang zu kommen. In acht Teile gegliedert (der letzte bildet den Anhang) behandeln Christian Nagel und seine Mitstreiter zunächst die Sprachgrundlagen, bevor sie kurz Visual Studio darstellen. Danach kommen die Basisbibliotheken an die Reihe, woran sich detaillierte Kapitel anschließen – ab circa der 800. Seite.

Linq, Windows Forms und die WPF, ASP.Net samt Ajax, die Communication sowie die Workflow Foundation sind allesamt berücksichtigt. Ob Hanser, Microsoft Press oder Wrox: Die Kaufentscheidung dürfte im Wesentlichen davon abhängen, in welcher Sprache jemand lesen will, welche Form der Herangehensweise sie vorzieht und wie viel er zu tragen bereit ist.

Alle drei Werke setzen auf .Net 3.5 auf. Zum .Net-Framework in dieser Version haben mehrere Verlage eigene Veröffentlichungen beigesteuert. So haben Jana Frank und Patrick A. Lorenz für Hanser „ASP.NET mit AJAX“ geschrieben, das, wie der Titel suggeriert, die Webprogrammierung mit dem derzeitigen Framework beinhaltet. Der in der von *iX*-Autor Holger Schwichtenberg herausgegebenen .Net-Bibliothek erschienene Band deckt tatsächlich nur den Webaspekt von .Net ab: ASP, Ajax inklusive Extensions, Javascript und das Control-Kit.

„Programming .NET 3.5“ von Jesse Liberty und Alex Horowitz hat O’Reilly im März in den USA veröffentlicht. Die Autoren haben nicht alle Bestandteile des Framework gleichwertig vorstellen wollen, sondern konzentrieren sich auf Präsentationstechniken wie WPF, Ajax, Silverlight et al. sowie SOA- und MVC-Aspekte. Kapitel zu Design Patterns Linq, die Workflow Foundation und Cardspace schließen den Band ab. Kein Werk für Einsteiger, aber laut den Autoren für Java-Kenner durchaus lesbar.

Noch spezialisierter geht Omar Al Zahir ans Framework heran. Sein „Building a Web 2.0 Portal with ASP.NET 3.5“ (Ende 2007 bei O’Reilly in den USA erschienen) kommt deshalb mit knapp 300 Seiten aus und eignet sich vor allem für an ASP.Net Gewöhnte. Im März dieses Jahres hat wiederum O’Reilly eine Neuauflage des 2003 erstmals veröffentlichten ADO.Net-Titels für das Framework 3.5 herausgebracht: Das „ADO.NET 3.5 Cookbook“ versammelt, wie in der Reihe üblich, eine gegliederte Rezeptsammlung für recht unterschiedliche Stolpersteine im Umgang mit der Software.

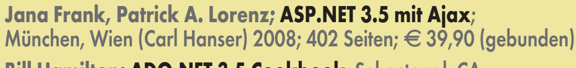
Ein Taschenratgeber von knapp 600 Seiten passt zwar in so manche Jackentasche, aber der zum IIS 7.0, Microsofts Webserver gehört eher ins Administratorenregal. William R. Stanek hat ihn für die Microsoft Press geschrieben; er bietet den Verwaltern und Entwicklern detaillierte Einsicht in die Arbeit mit dem IIS. Von der Konfiguration über diverse Module über Sicherheitsaspekte, Active Directory und SSL bis zur Leistungsüberwachung reicht die thematische Palette, wobei allein die Modulreferenz 170 Seiten einnimmt. Nachschlagegeeignet. *Henning Behme*

Jana Frank, Patrick A. Lorenz; ASP.NET 3.5 mit Ajax; München, Wien (Carl Hanser) 2008; 402 Seiten; € 39,90 (gebunden)

Bill Hamilton; ADO.NET 3.5 Cookbook; Sebastopol, CA (O’Reilly Media, Inc.) 2008; 2. Auflage; 995 Seiten; € 53,– (Paperback)

Jesse Liberty, Alex Horowitz; Programming .NET 3.5; Sebastopol, CA (O’Reilly Media, Inc.) 2008; 455 Seiten; € 43,– (Paperback)

Dirk Louis, Shinja Strasser; Microsoft Visual C# 2008; Grundlagen, Techniken, Profi-Know-how; Unterschleißheim (Microsoft Press) 2008; 1280 Seiten zzgl. DVD und CD-ROM; € 49,90 (gebunden)



Christian Nagel, Bill Evjen, Jay Glynn, Karli Watson, Morgan Skinner; Professional C# 2008; Indianapolis, IN (Wiley Publishing) 2008; 1782 Seiten; US-$ 59,99 (Paperback)

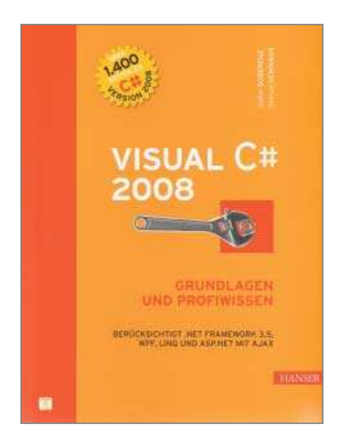
William R. Stanek; IIS 7.0; Taschenratgeber für Administratoren; München (Microsoft Press) 2008; 586 Seiten; € 34,90 (Paperback)

Omar Al Zahir; Building a Web 2.0 Portal with APS.NET 3.5; Sebastopol, CA (O’Reilly Media, Inc.) 2007; 290 Seiten; € 43,– (Paperback)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Thomas Gewinnus,
Walter Doberenz

Visual C# 2008

Grundlagen und Profiwissen

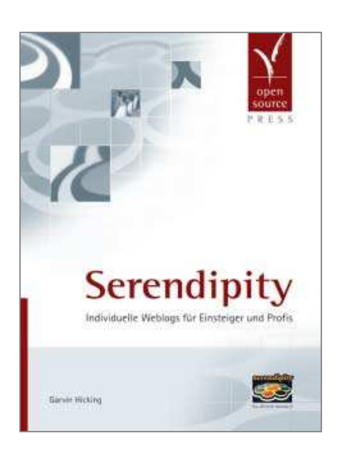
München 2008
Carl Hanser Verlag
1438 Seiten
59,90 €
ISBN 978-3-446-41440-2

Seit über 10 Jahren schreibt das Autorenteam Doberenz und Gewinnus Bücher für Programmierer und hat ganze Generationen von Borland-Delphi-, Visual-Basic- und nun Visual-C#-Entwicklern auf ihren Wegen begleitet. Das jetzt erschienene Werk vermittelt in pragmatischem Stil einen umfangreichen Wissensschatz rund um Visual C# 2008 und die aktuelle Version 3.5 des .Net-Framework. Dabei zielt das Buch auf praxisorientierte Entwickler, die Neues gerne anhand von Codebeispielen lernen. Nahezu jedes Sprachfeature veranschaulichen die Autoren. Dennoch soll dieses Buch keinen Ersatz für die Sprachreferenz darstellen, sondern hauptsächlich die Grundlagen vermitteln. So kommen nicht alle Collection-Klassen und Locking-Mechanismen vor, sondern nur die je wichtigsten. Dieses Wissen sollte allerdings genügen, um sich in der Onlinehilfe zu weiteren Techniken zu informieren.

Mit über 1400 Seiten ist der Umfang enorm und umfasst nahezu alle Themen, mit denen ein Entwickler in Berührung kommt. Der erste Teil beschäftigt sich mit den Grundlagen: der Entwicklungsumgebung Visual Studio sowie den grundlegenden Sprachfeatures sowie dem Umgang mit Dateien und XML. Ergänzt wird das Ganze durch Erläuterungen zu Fehlerbehandlung, LINQ, ADO.Net, Reflection und mehr. Der zweite Teil des Buches beschäftigt sich mit den Windows Forms – der Entwicklung grafischer Benutzeroberflächen. Hier finden sich neben der Erläuterung der Steuerelemente Kapitel zu Grafikprogrammierung, Komponentenentwicklung und Thread-Programmierung. Der dritte Teil behandelt die neue Präsentationsschnittstelle WPF, die die Entwicklung von Benutzeroberflächen revolutionieren soll. Der letzte Teil dreht sich um webbasierte Entwicklung mit ASP.Net; inklusive eines Ajax-Exkurses.

Das Layout ist übersichtlich, die Sprache spritzig, der Inhalt kurzweilig und durch viele Listings leicht verständlich. Auf eine CD-ROM hat der Verlag leider verzichtet, allerdings kann man alle Quelltexte von der Website der Autoren herunterladen. Einziges Manko: die Erläuterungen zur OOP. Etwas mehr Erklärungen wären gut gewesen. Darüber kann man allerdings angesichts der sonst hervorragenden Arbeit getrost hinwegsehen.

FLORIAN POTSCHKA



Garvin Hicking

Serendipity

Individuelle Weblogs für Einsteiger und Profis

München 2008
Open Source Press
751 Seiten
39,90 €
ISBN 978-3-937514-54-3

Dass „Blogging“ zur beliebten Freizeitbeschäftigung und zum Sprachrohr vieler Internet-Hobbyisten avanciert ist, liegt nicht zuletzt im reichhaltigen Softwareangebot begründet. Gratisanbieter versorgen Mitteilungsbedürftige mit einer meist werbefinanzierten Plattform – wer höhere Ansprüche stellt, kann auf Open-Source-Lösungen in praktisch jeder wichtigen Websprache zurückgreifen. Reicht der Leistungsumfang eines Wordpress nicht aus, gilt das in PHP geschriebene Serendipity als das Produkt der Wahl. Quasi die gesamte Prominenz der internationalen PHP greifen für ihre persönlichen Webtagebücher auf die quelloffene Software zurück und schätzen an dieser besonders die hohe Modularität, Standardkonformität und ihren zwar nicht makellosen, aber doch hohen Sicherheitsstandard.

Einer größeren Verbreitung stand jedoch die eher lückenhafte Dokumentation im Wege – ein Umstand, dem Garvin Hickings Werk nun Rechnung trägt. Das Buch ist als Handreichung für jeden Serendipity-Anwender konzipiert und deckt von der Installation und den ersten Schritten bis zur Erweiterung von „S9Y“ – so das modische Kürzel der Blog-Software – alle Bereiche ab.

Nachdem die grundlegenden Begriffe in der gebotenen Ausführlichkeit geklärt wurden, hilft Hickings Werk dem Neuling bei der Installation, die gerade bei restriktiven Shared-Hosting-Umgebungen einige Tücken bergen kann. Das eigentliche Weblog und der administrative Bereich sind Gegenstand der nächsten Abschnitte und werden auf insgesamt 120 Seiten so detailliert umschrieben, dass Ein- und Umsteiger den vollen Leistungsumfang der freien Blog-Software sofort nutzen können.

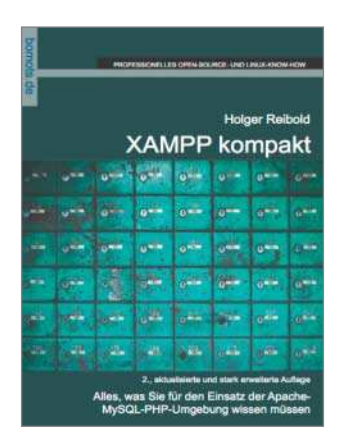
Eine mehrere Kapitel umfassende Übersicht listet alle verfügbaren Plug-ins auf und zeigt damit eine der Stärken von Serendipity: Durch seine Modularität ist S9Y für praktisch jede Blog-Variante einsetzbar und dank eines Online-Repository sind alle Plug-ins mit wenigen Klicks installierbar. Die hohe Volatilität bei den meist nicht vom Kernteam der Entwickler gewarteten Erweiterungen dürfte diese Liste jedoch bald veralten lassen.

Seine eigentliche Stärke entfaltet das Buch nach einem kurzen Zwischenspiel zu Wartung und Betrieb eines Blogs in der Entwicklerdokumentation. Hier findet der Nutzer alle notwendigen Informationen, um eigene Serendipity-Plug-ins oder neue Stilvorlagen zu entwickeln. Durch Wissen aus erster Hand kann Hicking hier punkten – ein Ausblick auf die Zukunft des Blogsystems rundet das Werk ab.

Insgesamt legt Garvin Hicking mit seinem Buch die detaillierte Dokumentation einer zu Unrecht als „ewiger Zweiter“ geltenden Software ab und wird ihr mit diesem Werk hoffentlich zu mehr Popularität bei allen Nutzergruppen verhelfen.

CHRISTOPHER KUNZ

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Holger Reibold

XAMPP kompakt

2., aktualisierte und stark erweitere Auflage
Saarbrücken 2008
Bomots Verlag
258 Seiten
19,80 €
ISBN 978-3-939316-35-0

Wer sich mit der Websoftwaresammlung XAMPP auseinandersetzen möchte, findet in dem kompakten Werk von Holger Reibold eine Einführung in die Installation des Pakets unter Linux und Windows bis hin zur ausführlichen Beschreibung seiner Komponenten – Apache, MySQL, PHP und Perl. Zunächst geht der Autor auf die Installation ein, wenn nötig stellt er die betriebssystemspezifischen Unterschiede heraus, ehe er sich den einzelnen Modulen in eigenen Kapiteln widmet. Beim Apache kommen dessen Konfigurationsdateien, Verzeichnisschutz mit *.htaccess*, sicherer SSL- und Webdav-Zugriff zu ihrem Recht. Der Autor verschweigt nicht, dass die Installation nur ein Dummy-SSL-Zertifikat enthält. Für einen Webshop mit SSL kommt man um den Erwerb bei einem Trustcenter nicht herum.

Reibold geht auf das im Open-Source-Bereich so verbreitete Datenbanksystem MySQL recht kurz ein, denn in einer solchen Einführung kann er so ein Thema nicht ausführlich behandeln. Immerhin stellt er zwei Tools vor, WinMySQLAdmin und MySQL Administrator. Ein eigenes Kapitel hat phpMyAdmin bekommen, in dem er gleich eine Datenbank und einige Beispieltabellen anlegt. Außerdem beschäftigt er sich mit FTP-Programmen: ProFTPD unter Unix (nur mit Cygwin unter Windows) und Filezilla von der Mozilla Foundation unter Windows.

Ein Kapitel geht auf die Sicherheit der XAMPP-Installation ein. Nicht nur das Absichern mit vernünftigen Datei- und Benutzerrechten, sondern auch Cross-Site Scripting und SQL-Injection kommen vor.

Das vorletzte Kapitel stellt die Einsatzgebiete dar: für das CMS Joomla oder Wordpress. Zu diesen hier nur angerissenen Themen bietet der Verlag andere Bücher an. Im letzten Kapitel versammelt Rebold Tipps und Tricks für den täglichen Einsatz von XAMPP. Im Windows-Abschnitt gibt der Autor unter anderem Tipps zu Schwierigkeiten mit dem SP2 bei XP oder mit Vista.

Abgeschlossen wird das Werk durch einen längeren Anhang, in dem sich Anmerkungen zu Add-ons finden. Fürs Herumspielen mit Webserver, DBMS und den Skriptsprachen eignet sich dieses Buch gut. Der Leser kann die Beispiele während einer Rechnersession gleich ausprobieren.

KARSTEN KISSER

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Urbanski, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Bianca Nagel (-456, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Die gewerbliche Nutzung abgedruckter Programme ist nur mit schriftlicher Genehmigung des Herausgebers zulässig.

Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über, Nachdruck nur mit Genehmigung des Verlages. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Sämtliche Veröffentlichungen in ***iX*** erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Printed in Germany

© Copyright 2008 by Heise Zeitschriften Verlag GmbH & Co. KG

ISSN 0935-9680



Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

November 2008



E-Mail-Warteschleifen fein dosiert

Greylisting gilt nach wie vor als wirksames Mittel gegen Spam, auch wenn es unter Mail-Administratoren berechtigte Bedenken dagegen gibt, da das Konzept einige Schwächen aufweist. Außerdem beginnen die Absender der Müllpost bereits, sich darauf einzustellen. Beidem können Mailserver-Betreiber durch ein erweiterbares, variables Greylisting begegnen, das nicht jede E-Mail aus unbekannter Quelle pauschal als verdächtig ansieht und ausbremst.

Neue Grundlage für Oracle Fusion

Knapp ein halbes Jahr nach der Übernahme von BEA hat Oracle den ersten Weblogic Server als Teil seiner Fusion Middleware vorgestellt. Das zugekaufte und angepasste Flaggschiff trägt den Namen 10gR3 und soll den selbst entwickelten Application Server ablösen. Umstiegswillige stehen nun vor der Frage, wie viel BEA noch in der neuen Oracle-Basis steckt.

**Heft 11/2008
erscheint am 16. Oktober 2008**

Es grünt in den Rechenzentren

Wer es nicht nur im eigenen Haus, sondern auch bei ausgelagerten Systemen und Diensten mit dem Stromsparen ernst meint, sollte sich seine Hoster und Provider genau ansehen. Was die nach dem heutigen Stand der Technik an Energiesparmaßnahmen betreiben und betreiben könnten, zeigt eine Marktübersicht über „Grüne Rechenzentren“.

Computer als Dolmetscher

Maschinelles Übersetzen von Texten gehört zu den älteren Projekten der Informationstechnik. Doch Computerlinguisten und Anhänger der Sprachstatistik wetteifern darum, wessen Ansatz der bessere ist. Zeit für eine Gegenüberstellung.



Semantische Notizen zu Bildern

Suchmaschinen finden seit einiger Zeit außer Texten auch Bilder. Ob der im Dateinamen vorkommende Ball ein Zeichen für ein Sportfoto oder ein Debütantinnentreffen ist, kann die Maschine allerdings nicht eruieren. RDF und Ontologiesprachen, wie das World Wide Web Consortium sie definiert, können bewirken, dass Fotos Metadaten über sich enthalten, was den Maschinen künftig weiterhelfen soll.

Kein wichtiges Thema mehr versäumen!
Die aktuelle iX-Inhaltsübersicht per E-Mail
Man verpasst ja sonst schon genug!
www.heise.de/bin/newsletter/listinfo/ix-inhalt

Das bringen





Netzwerk-Praxis: Erweitern, beschleunigen, effizienter verwalten

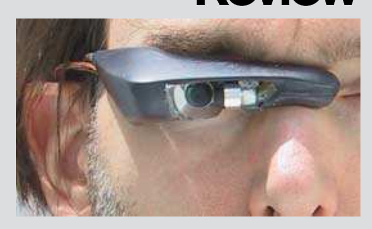
3D-Grafik: Radeon HD 4870 kontra Nvidia

26"-Monitore: Hohe Auflösung für wenig Geld

Audio-Editoren: Freeware kontra Profi-Software

Heft 20/08 jetzt am Kiosk

Technology Review
DAS M.I.T. - MAGAZIN FÜR INNOVATION



Nie wieder vergessen: Wie Lifelogger jeden Moment ihres Lebens aufzeichnen und dabei der Datenflut Herr werden.

Neue Formel für Feinkost: Molekulares Kochen dringt von der Spitzengastronomie in die Tiefkühlregale vor.

Heft 10/08 jetzt am Kiosk

TELEPOLIS
MAGAZIN DER NETZKULTUR



Hans Schmid: Das Plagiat, als eine schöne Kunst betrachtet – Poe, Pym und allerlei Kopisten

Marcus Hammerschmitt: „Ah, das Love-Ding!“ – Auf dem höchsten, schnellsten Punkt der Gegenwart: Monika Rinck

www.heise.de/tp/

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.